NEC

N8406-022A 1Gb Intelligent L2 Switch

Command Reference Guide (ISCLI)

Part number: 856-126757-306-00
First edition: July 2008

PN# 456-01767-000

Legal notices

© 2008 NEC Corporation

The information contained herein is subject to change without notice. The only warranties for NEC products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. NEC shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

SunOS™ and Solaris™ are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Part number: 856-126757-306-00

First edition: July 2008

Contents

ISCLI Reference
- Introduction 7
- Additional references 7
- Connecting to the switch 7
  - Establishing a console connection 7
  - Setting an IP address 8
  - Establishing a Telnet connection 8
  - Establishing an SSH connection 8
- Accessing the switch 9
- Idle timeout 10
- Typographical conventions 10

ISCLI basics
- Introduction 12
- Accessing the ISCLI 12
- ISCLI Command Modes 12
- Global commands 13
- Command line interface shortcuts 14
  - Command abbreviation 14
  - Tab completion 14

Information Commands
- Introduction 15
- System Information commands 16
- SNMPv3 Information commands 16
  - SNMPv3 USM User Table information 17
  - SNMPv3 View Table information 17
  - SNMPv3 Access Table information 18
  - SNMPv3 Group Table information 19
  - SNMPv3 Community Table information 19
  - SNMPv3 Target Address Table information 20
  - SNMPv3 Target Parameters Table information 20
  - SNMPv3 Notify Table information 21
  - SNMPv3 dump 22
- System information 23
- Show recent syslog messages 24
- System user information 24
- Layer 2 information 25
- FDB information commands 26
  - Show all FDB information 26
- Link Aggregation Control Protocol information 27
  - LACP dump 27
- Spanning Tree information 28
- Rapid Spanning Tree and Multiple Spanning Tree information 29
- Common Internal Spanning Tree information 31
- Trunk group information 33
- VLAN information 33
- Layer 3 information 34
- ARP information 34
  - Show all ARP entry information 35
  - ARP address list information 35
- IP information 35
- IGMP multicast group information 36
- IGMP multicast router port information 36
- RMON Information 36
  - RMON history information 36
  - RMON alarm information 37
  - RMON event information 38
- Link status information 39
- Port information 40
- Logical Port to GEA Port mapping 41
- Uplink Failure Detection information 42

Information dump 42

Statistics commands
Introduction 43
Port Statistics 43
Bridging statistics 44
Ethernet statistics 44
Interface statistics 46
Internet Protocol (IP) statistics 47
Link statistics 48
Port RMON statistics 48
Layer 2 statistics 50
FDB statistics 50
LACP statistics 50
Layer 3 statistics 51
IP statistics 51
ARP statistics 52
DNS statistics 53
ICMP statistics 53
TCP statistics 54
UDP statistics 55
IGMP Multicast Group statistics 56
GEA Layer 3 statistics 56
GEA Layer 3 statistics 56
Management Processor statistics 57
Packet statistics 57
TCP statistics 58
UDP statistics 58
CPU statistics 58
SNMP statistics 59
NTP statistics 61
Uplink Failure Detection statistics 62
Statistics dump 62

Configuration Commands
Introduction 63
Viewing and saving changes 63
Saving the configuration 63
System configuration 64
System host log configuration 65
Secure Shell Server configuration 66
RADIUS server configuration 67
TACACS+ server configuration 68
NTP server configuration 69
System SNMP configuration 70
SNMPv3 configuration 71
SNMPv3 User Security Model configuration 72
SNMPv3 View configuration 72
SNMPv3 View-based Access Control Model configuration 73
SNMPv3 Group configuration 73
SNMPv3 Community Table configuration 74
SNMPv3 Target Address Table configuration 74
SNMPv3 Target Parameters Table configuration 75
SNMPv3 Notify Table configuration 75
System Access configuration 76
Management Networks configuration 76
User Access Control configuration 77
User ID configuration 77
HTTPS Access configuration 78
Port configuration 79
Temporarily disabling a port 79
Port link configuration 80
Layer 2 configuration 80
Rapid Spanning Tree Protocol / Multiple Spanning Tree Protocol configuration 81
Common Internal Spanning Tree configuration 82
CIST bridge configuration 82

CIST port configuration ... 83
Spanning Tree configuration ... 84
Bridge Spanning Tree configuration ... 85
Spanning Tree port configuration ... 86
Forwarding Database configuration ... 87
Static FDB configuration ... 87
Trunk configuration ... 87
Layer 2 IP Trunk Hash configuration ... 88
Link Aggregation Control Protocol configuration ... 88
LACP Port configuration ... 89
VLAN configuration ... 89
Layer 3 configuration ... 90
IP interface configuration ... 90
Default Gateway configuration ... 91
Address Resolution Protocol configuration ... 91
IGMP configuration ... 92
IGMP snooping configuration ... 92
IGMP static multicast router configuration ... 93
IGMP filtering configuration ... 93
IGMP filter definition ... 93
IGMP filtering port configuration ... 94
Domain Name System configuration ... 94
Remote Monitoring configuration ... 95
RMON history configuration ... 95
RMON event configuration ... 95
RMON alarm configuration ... 96
Port mirroring ... 97
Port-based port mirroring ... 97
Uplink Failure Detection configuration ... 98
Failure Detection Pair configuration ... 98
Link to Monitor configuration ... 99
Link to Disable configuration ... 99
Configuration Dump ... 100
Saving the active switch configuration ... 100
Restoring the active switch configuration ... 100

Operations Commands
Introduction ... 101
Operations-level port options ... 101

Boot Options
Introduction ... 102
Updating the switch software image ... 102
Downloading new software to the switch ... 102
Selecting a software image to run ... 103
Uploading a software image from the switch ... 104
Selecting a configuration block ... 104
Resetting the switch ... 105
Accessing the AOS CLI ... 105
Current switch software information ... 105

Maintenance Commands
Introduction ... 106
System maintenance ... 106
Forwarding Database maintenance ... 106
Debugging options ... 107
ARP cache maintenance ... 107
IGMP Snooping maintenance ... 108
IGMP Mrouter maintenance ... 108
Technical support dump ... 108
FTP/TFTP technical support dump put ... 108
Uuencode flash dump ... 109
FTP/TFTP system dump put ... 109
Clearing dump information ... 109
Panic command ... 110
Unscheduled system dumps ... 110

ISCLI Reference

Introduction

The 1Gb Intelligent L2 Switch is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive switching software included in the switch provides a variety of options for accessing and configuring the switch:

- Text-based command line interfaces (AOS CLI and ISCLI) for access via a local terminal or remote Telnet/Secure Shell (SSH) session
- Simple Network Management Protocol (SNMP) support for access through network management software such as NEC WebSAM NetvisorPro
- A browser-based management interface for interactive network access through a Web browser

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Use a basic terminal to view information and statistics about the switch, and to perform any necessary configuration.

This guide describes how to use and configure on the Layer2 switch mode of the switch. The switch does not provide ISCLI on the SmartPanel.

This chapter explains how to access the ISCLI to the switch.

Additional references

Additional information about installing and configuring the switch is available in the following guides, which are attached in this product.

- *N8406-022A 1Gb Intelligent L2 Switch User's Guide*
- *N8406-022A 1Gb Intelligent L2 Switch Application Guide*
- *N8406-022A 1Gb Intelligent L2 Switch Command Reference Guide (AOS)*
- *N8406-022A 1Gb Intelligent L2 Switch Browser-based Interface Reference Guide*
- *N8406-022A 1Gb Intelligent L2 Switch SmartPanel Reference Guide*

Connecting to the switch

You can access the command line interface in one of the following ways:

- Using a console connection via the console port
- Using a Telnet connection over the network
- Using a Secure Shell (SSH) connection to securely log in over a network

Establishing a console connection

To establish a console connection with the switch, you need:

- A null modem cable with a female DB-9 connector (See the *User's Guide* for more information.)
- An ASCII terminal or a computer running terminal emulation software set to the parameters shown in the table below

Table 1 Console configuration parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

To establish a console connection with the switch:

1. Connect the terminal to the console port using the null modem cable.
2. Power on the terminal.
3. Press the Enter key a few times on the terminal to establish the connection.
4. You will be required to enter a password for access to the switch.

Setting an IP address

To access the switch via a Telnet or an SSH connection, you need to have an Internet Protocol (IP) address set for the switch. The switch can get its IP address in one of the following ways:

- Management port access:
  - Using a Dynamic Host Control Protocol (DHCP) server—When the `dhcp` client is `enabled`, the management interface (interface 256) requests its IP address from a DHCP server. The default value for the `dhcp` client is `enabled`.
  - Configuring manually—If the network does not support DHCP, you must configure the management interface (interface 256) with an IP address. If you want to access the switch from a remote network, you also must configure the management gateway (gateway 4).
- Uplink port access:
  - Using a Bootstrap Protocol (BOOTP) server—By default, the management interface is set up to request its IP address from a BOOTP server. If you have a BOOTP server on the network, add the Media Access Control (MAC) address of the switch to the BOOTP configuration file located on the BOOTP server. The MAC address can be found in the System Information menu (See the “System Information commands” section in the “Information Commands” chapter.) If you are using a DHCP server that also does BOOTP, you do not have to configure the MAC address.
  - Configuring manually—If the network does not support BOOTP, you must configure the management port with an IP address.

Establishing a Telnet connection

A Telnet connection offers the convenience of accessing the switch from any workstation connected to the network. Telnet provides the same options for user, operator, and administrator access as those available through the console port. By default, Telnet is enabled on the switch. The switch supports four concurrent Telnet connections.

Once the IP parameters are configured, you can access the ISCLI using a Telnet connection. To establish a Telnet connection with the switch, run the Telnet program on the workstation and enter the telnet command, followed by the switch IP address:

```
telnet <1Gb Intelligent L2 Switch IP address>
```

You will then be prompted to enter a password. The password determines the access level: administrator, operator, or user. See the “Accessing the switch” section later in this chapter for description of default passwords.

Establishing an SSH connection

Although a remote network administrator can manage the configuration of a switch via Telnet, this method does not provide a secure connection. The Secure Shell (SSH) protocol enables you to securely log into this switch over the network.

As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure. In order to use SSH, you must first configure it on the switch. See the “Secure Shell Server configuration” section in the “Configuration Commands” chapter for information on how to configure SSH.

The switch can perform only one session of key/cipher generation at a time. Therefore, an SSH/Secure Copy (SCP) client will not be able to log in if the switch is performing key generation at that time or if another client has just logged in before this client. Similarly, the system will fail to perform the key generation if an SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication—Client RSA authenticates the switch in the beginning of every connection
- Key Exchange—RSA
- Encryption:
  - AES256-CBC
  - AES192-CBC
  - AES128-CBC
  - 3DES-CBC
  - 3DES
  - ARCFOUR
- User Authentication—Local password authentication; Remote Authentication Dial-in User Service (RADIUS)

The following SSH clients are supported:

- SSH 3.0.1 for Linux (freeware)
- SecureCRT® 4.1.8 (VanDyke Technologies, Inc.)
- OpenSSH_3.9 for Linux (FC 3)
- FedoraCore 3 for SCP commands
- PuTTY Release 0.58 (Simon Tatham) for Windows

NOTE: This switch implementation of SSH is based on versions 1.5 and 2.0, and supports SSH clients from version 1.0 through version 2.0. SSH clients of other versions are not supported. You may configure the client software to use protocol SSH version 1 or version 2.

By default, SSH service is not enabled on the switch. Once the IP parameters are configured, you can access the ISCLI to enable SSH.

To establish an SSH connection with the switch, run the SSH program on the workstation by issuing the ssh command, followed by the user account name and the switch IP address:

```
>> # ssh <user>@<1Gb Intelligent L2 Switch IP address>
```

You will then be prompted to enter your password.

NOTE: The first time you run SSH from the workstation, a warning message might appear. At the prompt, enter yes to continue.

Accessing the switch

To enable better switch management and user accountability, this switch provides different levels or classes of user access. Levels of access to the CLI and Web management functions and screens increase as needed to perform various switch management tasks. The three levels of access are:

- User— Interaction with the switch is completely passive—nothing can be changed on this switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operator— Interaction with the switch is completely passive—nothing can be changed on this switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Administrator— Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reload/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on this switch. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique usernames and passwords. Once you are connected to the switch via the local console, Telnet, or SSH, you are prompted to enter a password. The password entered determines the access level. The default user names/password for each access level is listed in the following table.

NOTE: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see the “Setting passwords” section in the “First-time configuration” chapter.

Table 2 User access levels

User account	Description and tasks performed
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. The user account is enabled by default, and the default password is `user`.
Oper	The Operator has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. By default, the operator account is disabled and has no password.
Admin	The super user administrator has complete access to all command modes on the switch, including the ability to change both the user and administrator passwords. The admin account is enabled by default, and the default password is `admin`.

NOTE: With the exception of the admin user, access to each user level can be disabled by setting the password to an empty value.

Once you enter the administrator password and it is verified, you are given complete access to this switch.

Idle timeout

By default, this switch disconnects the console, Telnet, or SSH session after five minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. To change this parameter, see the “System configuration” section in the “Configuration Commands” chapter.

Typographical conventions

The following table describes the typographic styles used in this guide:

Typeface or symbol	Meaning
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets as you enter the command. Example: If the command syntax is **`ping <`***`IP address`***`>`** you enter `ping 192.32.10.12`
bold body text	Indicates objects, such as window names, icons, and user-interface objects, such as buttons and tabs.
`bold Courier text`	Indicates command names, options, and text that you must enter. Example: Use the **`show ip arp`** commands.
`plain Courier text`	Indicates command syntax and system output (for example: prompts and system messages). Example: `configure terminal`

braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.
	Example: If the command syntax is
	`show portchannel {<`*`1-12`***`>|hash|information}`**
	
	you must enter:
	`show portchannel <1-12>`
	
	or
	`show portchannel hash`
	
	or
	`show portchannel information`

Typeface or symbol	Meaning

brackets [ ]	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.
	Example: If the command syntax is
	show ip interface [<*1-256*>]
	
	you can enter
	`show ip interface`
	
	or
	`show ip interface 1`

italic text	Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by a hyphen. Example: If the command syntax is **show spanning-tree stp <***1-32***>** 1-32 represents a number between 1-32.

vertical line |	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.
	Example: If the command syntax is
	show portchannel {<*1-12***>|hash|information}**
	
	you must enter:
	`show portchannel <1-12>`
	
	or
	`show portchannel hash`
	
	or
	`show portchannel information`

ISCLI basics

Introduction

The ISCLI is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

This chapter describes the ISCLI Command Modes, and provides a list of commands and shortcuts that are commonly available from all the command modes within the ISCLI.

Accessing the ISCLI

The first time you start this switch, it boots into the AOS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

To access the AOS CLI, enter the following command from the ISCLI and reload the switch:

```
Switch(config)# boot cli-mode aos
```

The switch retains your CLI selection, even when you reset the configuration to factory defaults. The CLI boot mode is not part of the configuration settings.

ISCLI Command Modes

The ISCLI has three major command modes, listed in order of increasing privileges, as follows:

User EXEC mode: This is the initial mode of access. By default, password checking is disabled for this mode.

Privileged EXEC mode: The mode is accessed from User EXEC mode. If the Privileged EXEC password is enabled, you must enter a password to access Privileged EXEC mode.

Global Configuration mode: This mode allows you to make changes to the running configuration of the switch. If you save the configuration, the settings survive a reload of the switch. Several submodes are available within the Global Configuration mode (the following table for more information.

Each command mode provides a specific set of commands. The command set of each higher-privilege mode is a superset of the lower-privilege mode(s). All commands available in lower-lower-privilege modes are available in the higher-privilege modes.

The following table describes the ISCLI command modes.

Table 3 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit.
User EXEC `Switch>`	Default mode, entered automatically Exit: **`exit`** or **`logout`**
Privileged EXEC `Switch#`	Enter Privileged EXEC mode, from User EXEC mode: **`enable`** Exit to User EXEC mode: **`disable`** Quit ISCLI: **`exit`** or **`logout`**
Global configuration `Switch(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: **`configure terminal`** Exit to Privileged EXEC mode: **`end`** or **`exit`**
Port configuration `Switch(config-if)#`	Enter Port Configuration mode, from Global Configuration mode: **`interface gigabitethernet <`***`port number`***`>`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
VLAN configuration `Switch(config-vlan)#`	Enter VLAN Configuration mode, from Global Configuration mode: **`vlan <`***`1-4095`***`>`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Interface IP configuration `Switch(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: **`interface ip <`***`1-256`***`>`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 3 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit.
FDP configuration	Enter RIP Configuration mode, from Global Configuration mode: **`ufd fdp`** *<1-4>* Exit to Global Configuration mode: **`exit`**
`Switch(config-fdp)#`	Exit to Privileged EXEC mode: **`end`**

Global commands

Some basic commands are recognized throughout the ISCLI hierarchy. These commands are useful for obtaining online Help, navigating through the interface, and saving configuration changes. To get help about a specific command, type the command, followed by **`help`**.

The following table describes the global commands.

Table 4 Global commands

Command	Action
`?`	Provides more information about a specific command or lists commands available at the current level.
`exit`	Go up one level in the command-mode structure.
`copy running-config startup-config`	Write configuration changes to flash memory.
`exit or quit`	Exit from the command line interface and log out.
`ping`	Verify station-to-station connectivity across the network. The format is as follows: `ping` *<host name> | <IP address>* `[`*<number of tries>*`] [`*<msec delay>*`]` • IP address is the hostname or IP address of the device. • number of tries (optional) is the number of attempts (1-32). • msec delay (optional) is the number of milliseconds between attempts.
`traceroute`	Identifies the route used for station-to-station connectivity across the network. The format is as follows: `traceroute` *<host name> | <IP address>* `[`*<max-hops>*`] [`*<msec delay>*`]` • IP address is the hostname or IP address of the target station. • max-hops (optional) is the maximum distance to trace (1-16 devices) • msec delay (optional) is the number of milliseconds to wait for the response.
`telnet`	Allows you to Telnet out of the switch. The format is as follows: `telnet` *<host name> | <IP address>* `[`*<port number>*`]`
`show history`	Displays the 10 most recent commands.
`console-log`	Enables or disables console logs for the current session.
`who`	Displays a list of users who are currently logged in.

Command line interface shortcuts

The following shortcuts allow you to enter commands quickly and easily.

Command abbreviation

Most commands can be abbreviated by entering the first characters that distinguish the command from the others in the same mode. For example, consider the following full command:

```
Switch(config)# spanning-tree stp 1 bridge hello-time 2
```

The command shown above could also be entered as:

```
Switch(config)# sp stp 1 br h 2
```

Tab completion

Entering the first letter of a command at any prompt and press the Tab key to display all available commands or options that begin with that letter. Entering additional letters further refines the list of commands or options displayed.

If only one command fits the input text when you press the Tab key, that command is supplied on the command line, waiting to be entered.

Information Commands

Introduction

You can view configuration information for the switch in the ISCLI. This chapter discusses how to use the ISCLI to display switch information.

The following table describes general information commands.

Table 5 Information commands

Command	Usage
show sys-info	Displays system information. **Command mode**: All
show layer2 information	Displays Layer 2 information. **Command mode**: All
show layer3 information	Displays Layer 3 information. **Command mode**: All
show rmon	Displays Remote Monitoring Information. **Command mode**: All
show interface link	Displays configuration information about each port, including: • Port number • Port speed (10 Mb/s, 100 Mb/s, 1000 Mb/s, or any) • Duplex mode (half, full, or any) • Flow control for transmit and receive (no, yes, or any) • Link status (up or down) **Command mode**: All
show interface information	Displays port status information, including: • Port number • Whether the port uses VLAN tagging or not • Port VLAN ID (PVID) • Port name • VLAN membership **Command mode**: All
show geaport	Displays GEA port mapping information, used by service personnel. **Command mode**: All
show ufd	Displays Uplink Failure Detection information. **Command mode**: All
show information-dump	Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode**: All

System Information commands

The following table describes the System Information commands.

Table 6 System Information commands

Command	Usage
show snmp-server v3	Displays SNMP v3 information. **Command mode**: All
show sys-info	Displays system information, including: • System date and time • Switch model name and number • Switch name and location • MAC address of the switch management processor • IP address of IP interface #1 • Hardware version and part number • Software image file and version number • Configuration name • Log-in banner, if one is configured **Command mode**: All
show logging messages	Displays most recent syslog messages. **Command mode**: All
show access user	Displays User Access information. **Command mode**: All except User EXEC

SNMPv3 Information commands

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture, see RFC2271 to RFC2276.

The following table describes the SNMPv3 Information commands.

Table 7 SNMPv3 Information commands

Command	Usage
show snmp-server v3 user	Displays User Security Model (USM) table information. **Command mode**: All
show snmp-server v3 view	Displays information about view name, subtrees, mask and type of view. **Command mode**: All
show snmp-server v3 access	Displays View-based Access Control information. **Command mode**: All
show snmp-server v3 group	Displays information about the group that includes the security model, user name, and group name. **Command mode**: All
show snmp-server v3 community	Displays information about the community table. **Command mode**: All
show snmp-server v3 target-address	Displays the Target Address table. **Command mode**: All
show snmp-server v3 target-parameters	Displays the Target parameters table. **Command mode**: All
show snmp-server v3 notify	Displays the Notify table. **Command mode**: All
show snmp-server v3	Displays all the SNMPv3 information. **Command mode**: All

SNMPv3 USM User Table information

The following command displays SNMPv3 user information:

show snmp-server v3 user

Command mode: All

```
usmUser Table
User Name                       Protocol
------------------------------- --------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
```

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains information like:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol.

The following table describes the SNMPv3 User Table information.

Table 8 User Table parameters

Field	Description
`User Name`	This is a string that represents the name of the user that you can use to access the switch.
`Protocol`	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. switch software supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table information

The following command displays the SNMPv3 View Table:

show snmp-server v3 view

Command mode: All

```
View Name          Subtree                      Mask           Type
------------------ ---------------------------  -------------  --------
iso                  1                                        included
v1v2only             1                                        included
v1v2only             1.3.6.1.6.3.15                           excluded
v1v2only             1.3.6.1.6.3.16                           excluded
v1v2only             1.3.6.1.6.3.18                           excluded
```

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following table describes the SNMPv3 View Table information.

Table 9 View Table parameters

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of view subtrees is included or excluded from the MIB view.

SNMPv3 Access Table information

The following command displays SNMPv3 access information:

show snmp-server v3 access

Command mode: All

```
Group Name  Model   Level         ReadV     WriteV   NotifyV
----------  ------- ------------ --------- -------- -------
v1v2grp     snmpv1  noAuthNoPriv iso         iso     v1v2only
admingrp    usm     authPriv     iso         iso     iso
```

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view, and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following table describes the SNMPv3 Access Table information.

Table 10 Access Table parameters

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or auth-Priv.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table information

The following command displays SNMPv3 group information:

show snmp-server v3 group

Command mode: All

```
Sec Model  User Name                      Group Name
---------- ---------------------------- --------------------------------
snmpv1     v1v2only                     v1v2grp
usm        adminmd5                     admingrp
usm        adminsha                     admingrp
```

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following table describes the SNMPv3 Group Table information.

Table 11 Group Table parameters

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the user.
Group Name	Displays the access name of the group.

SNMPv3 Community Table information

The following command displays SNMPv3 community information:

show snmp-server v3 community

Command mode: All

```
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
trap1      public     v1v2only             v1v2trap
```

This command displays the community table information stored in the SNMP engine.

The following table describes the SNMPv3 Community Table information.

Table 12 Community Table information

Field	Description
Index	Displays the unique index value of a row in this table.
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

SNMPv3 Target Address Table information

The following command displays SNMPv3 target address information:

show snmp-server v3 target-address

Command mode: All

```
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
trap1      47.81.25.66     162  v1v2trap   v1v2param
```

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

The following table describes the SNMPv3 Target Address Table information.

Table 13 Target Address Table information

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

SNMPv3 Target Parameters Table information

The following command displays SNMPv3 target parameters information:

show snmp-server v3 target-parameters

Command mode: All

```
Name                MP Model User Name            Sec Model Sec Level
------------------- -------- -------------------- --------- -----------
v1v2param            snmpv2c  v1v2only             snmpv1    noAuthNoPriv
```

The following table describes the SNMPv3 Target Parameters Table information.

Table 14 Target Parameters Table information

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargeParamsEntry.
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the securityName, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an inconsistentValue error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table information

The following command displays the SNMPv3 Notify Table:

`show snmp-server v3 notify`

Command mode: All

```
Name                 Tag
-------------------- --------------------
v1v2trap             v1v2trap
```

The following table describes the SNMPv3 Notify Table information.

Table 15 SNMPv3 Notify Table information

Field	Description
`Name`	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry.
`Tag`	This represents a single tag value which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry is selected. If this entry contains a value of zero length, no entries are selected.

SNMPv3 dump

The following command displays SNMPv3 information:

`show snmp-server v3`

Command mode: All

```
Engine ID = 80:00:07:50:03:00:0F:6A:F8:EF:00
usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
admin                           NO AUTH, NO PRIVACY
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH, NO PRIVACY

vacmAccess Table:
Group Name Model   Level        ReadV   WriteV   NotifyV
---------- ------- ------------ ------- -------- ------
admin      usm     noAuthNoPriv org     org      org
v1v2grp    snmpv1  noAuthNoPriv org     org      v1v2only
admingrp   usm     authPriv     org     org      org

vacmViewTreeFamily Table:
View Name            Subtree         Mask         Type
-------------------- --------------- ------------ --------------
org                  1.3                          included
v1v2only             1.3                          included
v1v2only             1.3.6.1.6.3.15               excluded
v1v2only             1.3.6.1.6.3.16               excluded
v1v2only             1.3.6.1.6.3.18               excluded

vacmSecurityToGroup Table:
Sec Model  User Name                       Group Name
---------- ------------------------------- ----------------------
snmpv1     v1v2only                        v1v2grp
usm        admin                           admin
usm        adminsha                        admingrp

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------

snmpNotify Table:
Name                 Tag
-------------------- --------------------

snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------

snmpTargetParams Table:
Name                 MP Model User Name          Sec Model Sec Level
-------------------- -------- ------------------ --------- -------
```

System information

The following command displays system information:

`show sys-info`

Command mode: All

```
System Information at  6:56:22 Thu Jan 11, 2006
Time zone: Asia/Tokyo

Blade Network Technologies 1Gb Intelligent L2 Switch
sysName:
sysLocation:
RackId: NEC01A 6X00125
RackName: Default_Rack_Name
EnclosureSerialNumber: NEC01A 6X00125
EnclosureName: Default_Chassis_Name
BayNumber:  1

Switch is up 0 days, 14 hours, 56 minutes and 22 seconds.
Last boot reason: reset from console

MAC address: 00:10:00:01:00:01    IP (If 1) address: 10.14.4.16
Revision:
Switch Serial No:
Hardware Part No:                 Spare Part No:
Software Version 1.2.0 (FLASH image1), active configuration.
```

System information includes:

- System date and time
- Switch model name and number
- Rack name and location
- MAC address of the switch management processor
- IP address of the switch
- Software image file and version number
- Current configuration block (active, backup, or factory default)
- Login banner, if one is configured

Show recent syslog messages

The following command displays system log messages:

`show logging messages`

Command mode: All

```
Date   Time            Severity level                  Message
----   ----         -----------------                  -------
Jul 8 17:25:41             NOTICE              system: link up on port 1
Jul 8 17:25:41             NOTICE              system: link up on port 8
Jul 8 17:25:41             NOTICE              system: link up on port 7
Jul 8 17:25:41             NOTICE              system: link up on port 12
Jul 8 17:25:41             NOTICE              system: link up on port 11
Jul 8 17:25:41             NOTICE              system: link up on port 14
Jul 8 17:25:41             NOTICE              system: link up on port 13
Jul 8 17:25:41             NOTICE              system: link up on port 16
Jul 8 17:25:41             NOTICE              system: link up on port 15
Jul 8 17:25:41             NOTICE              system: link up on port 17
Jul 8 17:25:41             NOTICE              system: link up on port 20
Jul 8 17:25:41             NOTICE              system: link up on port 22
Jul 8 17:25:41             NOTICE              system: link up on port 23
Jul 8 17:25:41             NOTICE              system: link up on port 21
Jul 8 17:25:42             NOTICE              system: link up on port 4
Jul 8 17:25:42             NOTICE              system: link up on port 3
Jul 8 17:25:42             NOTICE              system: link up on port 6
Jul 8 17:25:42             NOTICE              system: link up on port 5
Jul 8 17:25:42             NOTICE              system: link up on port 10
Jul 8 17:25:42             NOTICE              system: link up on port 9
```

Each message contains a date and time field and has a severity level associated with it. One of eight different prefixes is used to indicate the condition:

- EMERG—indicates the system is unusable
- ALERT—indicates action should be taken immediately
- CRIT—indicates critical conditions
- ERR—indicates error conditions or eroded operations
- WARNING—indicates warning conditions
- NOTICE—indicates a normal but significant condition
- INFO—indicates an information message
- DEBUG—indicates a debug-level message

System user information

The following command displays user status information:

`show access user`

Command mode: All except User EXEC

```
Usernames:
  user     - enabled
  oper     - disabled
  admin    - Always Enabled

Current User ID table:
  1: name tech1   , ena, cos user    , password valid, online
  2: name tech2   , ena, cos user    , password valid, offline
```

The following table describes the user status information.

Table 16 User status Information

Field	Usage
`user`	Displays the status of the `user` access level.
`oper`	Displays the status of the `oper` (operator) access level.
`admin`	Displays the status of the `admin` (administrator) access level.
`Current User ID Table`	Displays the status of configured user IDs.

Layer 2 information

The following table describes the Layer 2 Information commands. The following sections provide more detailed information and commands.

Table 17 Layer 2 information commands

Command	Usage
show mac-address-table	Displays Forwarding Database Information. **Command mode:** All
show spanning-tree stp *<1-32>* **information**	In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information: • Priority • Hello interval • Maximum age value • Forwarding delay • Aging time You can also refer to the following port-specific STP information: • Port number and priority • Cost • State **Command mode:** All
show spanning-tree mstp cist information	Displays Common internal Spanning Tree (CIST) bridge information, including the following: • Priority • Hello interval • Maximum age value • Forwarding delay You can also view port-specific CIST information, including the following: • Port number and priority • Cost • State **Command mode:** All
show portchannel information	When trunk groups are configured, you can view the state of each port in the various trunk groups. **Command mode:** All
show vlan information	Displays VLAN configuration information, including: • VLAN Number • VLAN Name • Status • Port membership of the VLAN **Command mode:** All
show layer2 information	Dumps all switch information available from Layer 2 memory (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

FDB information commands

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

NOTE: The master forwarding database supports up to 8K MAC address entries on the management processor (MP) per switch.

Table 18 FDB information commands

show mac-address-table address *<mac-address>*	Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format: xx:xx:xx:xx:xx:xx. (For example: 08:00:20:12:34:56) You can also enter the MAC address using the format: xxxxxxxxxxxx. (For example: 080020123456) **Command mode:** All
show mac-address-table port *<port number>*	Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table vlan *<1-4095>*	Displays all FDB entries on a single VLAN. The range is 1-4095. **Command mode:** All
show mac-address-table state {forward|trunk|unknown}	Displays all FDB entries that match a particular state. **Command mode:** All
show mac-address-table	Displays all entries in the Forwarding Database. **Command mode:** All

Show all FDB information

The following command displays Forwarding Database information:

show mac-address-table

Command mode: All

```
   MAC address      VLAN  Port  Trnk  State
-----------------  ----  ----  ----  -----
00:02:01:00:00:00   300          1    TRK
00:02:01:00:00:01   300   23           FWD
00:02:01:00:00:02   300   23           FWD
00:02:01:00:00:03   300   23           FWD
00:02:01:00:00:04   300   23           FWD
00:02:01:00:00:05   300   23           FWD
00:02:01:00:00:06   300   23           FWD
00:02:01:00:00:07   300   23           FWD
00:02:01:00:00:08   300   23           FWD
00:02:01:00:00:09   300   23           FWD
00:02:01:00:00:0a   300   23           FWD
00:02:01:00:00:0b   300   23           FWD
00:02:01:00:00:0c   300   23           FWD
```

An address that is in the forwarding (FWD) state indicates that the switch has learned it. When in the trunking (TRK) state, the Trnk field displays the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated.

Clearing entries from the forwarding database

To delete a static MAC address from the forwarding database (FDB), see the “Static FDB configuration” section in the “Configuration Commands” chapter.

Link Aggregation Control Protocol information

The following table describes the Link Aggregation Control Protocol information commands.

Table 19 LACP information commands

Command	Usage
show interface gigabitEthernet <*port number***> lacp information**	Displays LACP aggregator information for the port. **Command mode**: All
show lacp	Displays LACP information for the port. **Command mode**: All
show lacp information	Displays all LACP information parameters. **Command mode**: All

LACP dump

The following command displays LACP information:

show lacp information

Command mode: All

```
>> LACP# dump
port  lacp      adminkey  operkey  selected    prio    attached  trunk
                                                        aggr
------------------------------------------------------------------------
   1  off             1        1         n    32768        --     --
   2  off             2        2         n    32768        --     --
   3  off             3        3         n    32768        --     --
   4  off             4        4         n    32768        --     --
   5  off             5        5         n    32768        --     --
   6  off             6        6         n    32768        --     --
   7  off             7        7         n    32768        --     --
   8  off             8        8         n    32768        --     --
```

LACP dump includes the following information for each port in the switch:

- lacp—Displays the port's LACP mode (active, passive, or off)
- adminkey—Displays the value of the port's adminkey.
- operkey—Shows the value of the port's operational key.
- selected—Indicates whether the port has been selected to be part of a Link Aggregation Group.
- prio—Shows the value of the port priority.
- attached aggr—Displays the aggregator associated with each port.
- trunk—This value represents the LACP trunk group number.

Spanning Tree information

The following table describes the Spanning Tree Protocol (STP) information commands.

Table 20 STP information commands

Command	Usage
show spanning-tree stp *<1-32>*	Displays information about the spanning tree group. **Command mode**: All
show spanning-tree stp *<1-32>* **bridge**	Displays STP bridge information. **Command mode**: All
show spanning-tree stp *<1-32>* **information**	Displays STP information. **Command mode**: All
show spanning-tree	Displays all STP information. **Command mode**: All

The following command displays Spanning Tree information:

show spanning-tree

Command mode: All

```
----------------------------------------------------------------------

upfast disabled, update 40

----------------------------------------------------------------------


Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1

Current Root:             Path-Cost    Port  Hello MaxAge FwdDel
 8000 00:02:a5:d1:0f:ed         8       20    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      2      20      15     300

Port  Priority   Cost   FastFwd    State       Designated Bridge     Des Port
----  --------   ----   --------  ----------   --------------------- -------
  1          0      0       n      FORWARDING *
  2          0      0       n      FORWARDING *
  3          0      0       n      FORWARDING *
```

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If RSTP/MSTP is turned on, see the “Rapid Spanning Tree information” section for Spanning Tree Group information. In addition to seeing if STP is enabled or disabled, you can view the following STP bridge information:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path cost
- Port
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific STP information:

- Port number and priority
- Cost
- State
- Port Fast Forwarding state
- Designated bridge
- Designated port

The following table describes the STP parameters.

Table 21 STP parameters

Parameter	Description
Current Root	Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root.
Path-Cost	Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge).
Port	The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost.
State	The State field shows the current state of the port. The State field can be one of the following: BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
Designated bridge	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
Designated port	The port ID of the port on the Designated Bridge to which this port is connected.

Rapid Spanning Tree and Multiple Spanning Tree information

The following command displays RSTP/MSTP information:

show spanning-tree

Command mode: All

```
------------------------------------------------------------------

upfast disabled, update 40

------------------------------------------------------------------

Spanning Tree Group 1: On (RSTP)
VLANs: 1-3 4095

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8000 00:00:01:00:19:00        0       0    9     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      9      20      15     300

Port  Prio  Cost   State  Role    Designated Bridge   Des Port  Type
----  ----  ----  ------  ----  --------------------- --------  ----
  1     0       0     DSB
  2     0       0     DSB
  3     0       0     DSB
  4     0       0     DSB
  5     0       0     DSB
  6     0       0     DSB
  7     0       0     DSB
  8     0       0     DSB
  9     0       0     DSB
 10     0       0     DISC
 11     0       0     FWD   DESG 8000-00:00:01:00:19:00   8017  P2P2,Edge
 12     0       0     FWD   DESG 8000-00:00:01:00:19:00   8018  P2P
```

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on, you can view the following RSTP bridge information for the Spanning Tree Group:

- Status of Uplink Fast (upfast)
- Current root MAC address
- Path-Cost
- Port
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also refer to the following port-specific RSTP information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Link type

The following table describes the STP parameters in RSTP or MSTP mode.

Table 22 Rapid Spanning Tree parameter descriptions

Parameter	Description
`Current Root`	Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root.
`Path-Cost`	Path-cost is the total path cost to the root bridge. It is the summation of the path cost between bridges (up to the root bridge).
`Port`	The current root port refers to the port on the switch that receives data from the current root. Zero (0) indicates the root bridge of the STP.
`Priority (bridge)`	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
`Hello`	The hello time parameter specifies, in seconds, how often the root bridge transmits a configurationbridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
`MaxAge`	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
`FwdDel`	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
`Aging`	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
`Priority (port)`	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
`Cost`	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated.
`State`	Shows the current state of the port. The State field in RSTP/MSTP mode can be one of the following: `Discarding (DISC)`, `Learning (LRN)`, `Forwarding (FWD)`, or `Disabled (DSB)`.
`Role`	Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST), or Unknown (UNK).
`Designated bridge`	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
`Designated port`	The port ID of the port on the Designated Bridge to which this port is connected.
`Type`	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

Common Internal Spanning Tree information

The following command displays Common Internal Spanning Tree (CIST) information:

`show spanning-tree mstp cist information`

Command mode: All

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62
Common Internal Spanning Tree:
VLANs: 1 3-4094

Current Root:            Path-Cost  Port   MaxAge   FwdDel
 8000 00:03:42:fa:3b:80      11     1       20      15

CIST Regional Root:    Path-Cost
 8000 00:03:42:fa:3b:80       11

Parameters:  Priority  MaxAge  FwdDel  Hops
               32768      20      15    20

Port Prio Cost State  Role Designated Bridge     Des Port Hello Type
---- ---- ---- ------ ---- -------------------- -------- ----- ----
  1  128  2000   FWD  DESG 8000-00:03:42:fa:3b:80  8001    4  P2P, Edge
  2  128  2000   FWD  DESG 8000-00:03:42:fa:3b:80  8002
  3  128  2000   DSB
  4  128  2000   DSB
  5  128  2000   DSB
  6  128  2000   DSB
  7  128  2000   DSB
  8  128  2000   DSB
  9  128  2000   DSB
 10  128  0      DSB
 11  128  2000   FWD   DESG 8000-00:03:42:fa:3b:80
 12  128  2000   DSB
```

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

- CIST root
- CIST regional root
- Priority
- Maximum age value
- Forwarding delay
- Hops

You can also refer to the following port-specific CIST information:

- Port number and priority
- Cost
- State
- Role
- Designated bridge and port
- Hello interval
- Link type and port type

The following table describes the CIST parameters.

Table 23 Common Internal Spanning Tree parameter descriptions

Parameter	Description
`CIST Root`	Shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
`CIST Regional Root`	Shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
`Priority (bridge)`	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
`MaxAge`	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
`FwdDel`	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
`Hops`	Shows the maximum number of bridge hops allowed before a packet is dropped.
`Priority (port)`	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
`Cost`	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of zero (0) indicates that the cost will be set to the appropriate default after the link speed has been auto-negotiated.
`State`	Shows the current state of the port. The state field can be one of the following: `Discarding (DISC)`, `Learning (LRN)`, `Forwarding` (FWD), or `Disabled (DSB)`.
`Role`	Shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Master (MAST), or Unknown (UNK).
`Designated Bridge`	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
`Designated Port`	The port ID of the port on the Designated Bridge to which this port is connected. Information includes the port priority (hex) and the port number (hex).
`Hello`	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
`Type`	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

Trunk group information

The following command displays Trunk Group information:

show portchannel information

Command mode: All

```
Trunk group 1, Enabled
port state:
  17: STG  1 forwarding
  18: STG  1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

NOTE: If Spanning Tree Protocol on any port in the trunk group is set to forwarding, the remaining ports in the trunk group are set to forwarding.

VLAN information

The following table describes the VLAN information commands.

Table 24 VLAN information commands

Command	Usage
show vlan	Displays VLAN information **Command mode**: All
show vlan information	Displays VLAN information, including spanning tree assignment. **Command mode**: All

The following command displays VLAN information:

show vlan information

Command mode: All

```
VLAN                Name                Status  Ports
----  --------------------------------- ------  ----------------
1     Default VLAN                        ena    4  5
2     pc03p                               ena    2
7     pc07f                               ena    7
11    pc04u                               ena    11
14    8600-14                             ena    14
15    8600-15                             ena    15
16    8600-16                             ena    16
17    8600-17                             ena    17
18    35k-1                               ena    18
19    35k-2                               ena    19
20    35k-3                               ena    20
21    35k-4                               ena    21
22    pc07z                               ena    22
24    redlan                              ena    24
300   ixiaTraffic                         ena    1 12 13 23
4000  bpsports                            ena    3-6 8-10
4095  Mgmt VLAN                           dis    empty
```

This information display includes all configured VLANs and all member ports that have an active link state.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN

Layer 3 information

The following table describes basic Layer 3 Information commands. The following sections provide more detailed information and commands. Layer 3 functionality is limited in this release.

Table 25 Layer 3 information commands

Command	Usage
show ip arp	Displays Address Resolution Protocol (ARP) Information. **Command mode:** All except User EXEC
show layer3 information	Displays IP Information. IP information, includes: • IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. • Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status • IP forwarding information: Enable status, Inet and Imask • Port status **Command mode:** All except User EXEC
show ip igmp groups	Displays IGMP Information. **Command mode:** All except User EXEC
show layer3	Dumps all switch information available from Layer 3 memory (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All except User EXEC

ARP information

The Address Resolution Protocol (ARP) information includes IP address and MAC address of each entry, address status flags, VLAN, and port for the address, and port referencing information.

The following table describes the Address Resolution Protocol commands.

Table 26 ARP information

Command	Usage
show ip arp find *<IP address>*	Displays a single ARP entry by IP address. **Command mode:** All except User EXEC
show ip arp interface *<port number>*	Displays the ARP entries on a single port. **Command mode:** All except User EXEC
show ip arp vlan *<1-4095>*	Displays the ARP entries on a single VLAN. **Command mode:** All except User EXEC
show ip arp	Displays all ARP entries, including: • IP address and MAC address of each entry • Address status flag • The VLAN and port to which the address belongs The ports which have referenced the address (empty if no port has routed traffic to the IP address shown) **Command mode:** All except User EXEC
show ip arp reply	Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags. **Command mode:** All except User EXEC

Show all ARP entry information

The following command displays ARP information:

show ip arp

Command mode: All except User EXEC

```
IP address      Flags     MAC address              VLAN      Port
--------------- -----    -----------------         ----      ----
192.168.2.4             00:50:8b:b2:32:cb          1         18
192.168.2.19            00:0e:7f:25:89:b5          1         17
192.168.2.61    P       00:0f:6a:ed:46:00          1
```

The Flag field provides additional information about an entry. If no flag displays, the entry is normal.

Table 27 ARP dump flag parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

ARP address list information

The following command displays ARP address list information:

show ip arp reply

Command mode: All except User EXEC

```
  IP address        IP mask        MAC address     VLAN Flags
--------------- ---------------  ----------------- ---- -----
205.178.18.66   255.255.255.255  00:70:cf:03:20:04 4095
205.178.50.1    255.255.255.255  00:70:cf:03:20:06    1
```

This screen displays all entries in the ARP cache.

IP information

The following command displays Layer 3 information:

show layer3 information

Command mode: All

```
Interface information:
  1: 47.80.23.243    255.255.254.0   47.80.23.255,    vlan 1, up
Default gateway information: metric strict
  1: 47.80.22.1,      up
  2: 47.80.225.2,     up
```

The following interface and default gateway information is displayed:

- Interface number
- IP address
- IP mask
- IP broadcast address
- Operational status

IGMP multicast group information

The following table describes the commands used to display information about IGMP groups learned by the switch.

Table 28 IGMP Multicast Group commands

Command	Usage
show ip igmp groups address *<IP address>*	Displays a single IGMP multicast group by its IP address. **Command mode:** All except User EXEC
show ip igmp groups vlan *<1-4094>*	Displays all IGMP multicast groups on a single VLAN. **Command mode:** All except User EXEC
show ip igmp groups interface *<port number>*	Displays all IGMP multicast groups on a single port. **Command mode:** All except User EXEC
show ip igmp groups trunk *<1-40>*	Displays all IGMP multicast groups on a single trunk group. **Command mode:** All except User EXEC
show ip igmp groups	Displays information for all multicast groups. **Command mode:** All except User EXEC

IGMP multicast router port information

The following table describes the commands used to display information about multicast routers learned through IGMP Snooping.

Table 29 IGMP Multicast Router information commands

Command	Usage
show ip igmp mrouter vlan *<1-4094>*	Displays information for all multicast groups on a single VLAN. **Command mode:** All except User EXEC
show ip igmp mrouter information	Displays information for all multicast groups learned by the switch. **Command mode:** All except User EXEC

RMON Information

The following command displays general RMON information:

show rmon

Command mode: All

RMON history information

The following command displays RMON history information:

show rmon history

Command mode: All

```
RMON History group configuration:

Index                IFOID               Interval  Rbnum  Gbnum
-----  -------------------------------  --------  -----  -----
    1          1.3.6.1.2.1.2.2.1.1.24        30      5      5
    2          1.3.6.1.2.1.2.2.1.1.24        30      5      5
    3          1.3.6.1.2.1.2.2.1.1.18        30      5      5
    4          1.3.6.1.2.1.2.2.1.1.19        30      5      5
    5          1.3.6.1.2.1.2.2.1.1.24      1800      5      5
```

The following table describes the RMON History Information parameters.

Table 30 RMON History Information

Command	Usage
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.

RMON alarm information

The following command displays RMON alarm information:

show rmon alarm

Command mode: All

```
RMON Alarm group configuration:

Index  Interval  Type   rLimit    fLimit   rEvtIdx  fEvtIdx  last value
-----  --------  ----  --------  --------  -------  -------  ----------
    1        30   abs        10         0        1        0           0
    2       900   abs         0        10        0        2           0
    3       300   abs        10        20        0        0           0
    4      1800   abs        10         0        1        0           0
    5      1800   abs        10         0        1        0           0
    8      1800   abs        10         0        1        0    56344540
   10      1800   abs        10         0        1        0           0
   11      1800   abs        10         0        1        0           0
   15      1800   abs        10         0        1        0           0
   18      1800   abs        10         0        1        0           0
  100      1800   abs        10         0        1        0           0

Index               OID
-----  ------------------------------
    1        1.3.6.1.2.1.2.2.1.10.257
    2        1.3.6.1.2.1.2.2.1.11.258
    3        1.3.6.1.2.1.2.2.1.12.259
    4        1.3.6.1.2.1.2.2.1.13.260
    5        1.3.6.1.2.1.2.2.1.14.261
    8        1.3.6.1.2.1.2.2.1.10.280
   10        1.3.6.1.2.1.2.2.1.15.262
   11        1.3.6.1.2.1.2.2.1.16.263
   15        1.3.6.1.2.1.2.2.1.19.266
   18        1.3.6.1.2.1.2.2.1.10.279
  100        1.3.6.1.2.1.2.2.1.17.264
```

The following table describes the RMON Alarm Information parameters.

Table 31 RMON Alarm Information

Command	Usage
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Type	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: abs: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. delta: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
rEvtIdx	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
fEvtIdx	Displays the falling alarm event index that is triggered when a falling threshold is crossed.
Last value	Displays the last sampled value.
OID	Displays the MIB Object Identifier for each alarm index.

RMON event information

The following command displays RMON event information:

`show rmon event`

Command mode: All

```
RMON Event group configuration:

Index  Type     Last Sent                Description
-----  ----  ----------------  ---------------------------------
    1  both    0D: 0H: 1M:20S   Event_1
    2  none    0D: 0H: 0M: 0S   Event_2
    3   log    0D: 0H: 0M: 0S   Event_3
    4  trap    0D: 0H: 0M: 0S   Event_4
    5  both    0D: 0H: 0M: 0S   Log and trap event for Link Down
   10  both    0D: 0H: 0M: 0S   Log and trap event for Link Up
   11  both    0D: 0H: 0M: 0S   Send log and trap for icmpInMsg
   15  both    0D: 0H: 0M: 0S   Send log and trap for icmpInEchos
  100  both    0D: 0H: 0M: 0S   Event_100
```

The following table describes the RMON Event Information parameters.

Table 32 RMON Event Information

Command	Usage
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: log, trap, both.
Last Sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.

Link status information

The following command displays link information:

`show interface link`

Command mode: All

```
------------------------------------------------------------------------
Port   Speed    Duplex     Flow Ctrl      Link
----   -----   --------  --TX-----RX--   ------
  1    1000       any     yes    yes      down
  2    1000       any     yes    yes      down
  3    1000       full    yes    yes      down
  4    1000       full    yes    yes      down
  5    1000       any     yes    yes      down
  6    1000       any     yes    yes      down
  7    1000       any     yes    yes      down
  8    1000       full    yes    yes       up
  9    1000       full    yes    yes      down
 10    1000       full    yes    yes      down
 11    1000       any     yes    yes      down
 12    1000       any     yes    yes      down
 13    1000       any     yes    yes      down
 14    1000       any     yes    yes      down
 15    1000       any     yes    yes      down
 16    1000       any     yes    yes      down
 17    1000       full    yes    yes       up
 18    1000       full    yes    yes       up
 19    100        full    yes    yes       up
 20    100        full    yes    yes      down
 21    1000       full    yes    yes      down
 22    1000       full    no     yes      down
 23    any        any     yes    yes      down
 24    any        any     yes    yes      down
```

Use this command to display link status information about each port on a switch, including:

- Port number
- Port speed (10 Mb/s, 100 Mb/s, 1000 Mb/s, or any)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no, yes, or any)
- Link status (up or down)

Port information

The following command displays port information:

`show interface information`

Command mode: All

```
Port Tag RMON PVID      NAME                 VLAN(s)
---- --- ---- ---- -------------- --------------------------------
  1   n   d       1 Downlink1      1
  2   n   d       1 Downlink2      1
  3   n   d       1 Downlink3      1
  4   n   d       1 Downlink4      1
  5   n   d       1 Downlink5      1
  6   n   d       1 Downlink6      1
  7   n   d       1 Downlink7      1
  8   n   d       1 Downlink8      1
  9   n   d       1 Downlink9      1
 10   n   d       1 Downlink10     1
 11   n   d       1 Downlink11     1
 12   n   d       1 Downlink12     1
 13   n   d       1 Downlink13     1
 14   n   d       1 Downlink14     1
 15   n   d       1 Downlink15     1
 16   n   d       1 Downlink16     1
 17   n   d       1 Xconnect1      1
 18   n   d       1 Xconnect2      1
 19   n   d    4095 Mgmt           4095
 20   n   d       1 Uplink1        1
 21   n   d       1 Uplink2        1
 22   n   d       1 Uplink3        1
 23   n   d       1 Uplink4        1
 24   n   d       1 Uplink5        1
```

Port information includes:

- Port number
- Whether the port uses VLAN tagging or not (y or n)
- Whether Remote Monitoring (RMON) is enabled or disabled (e or d)
- Port VLAN ID (PVID)
- Port name
- VLAN membership

Logical Port to GEA Port mapping

The following command displays information about GEA ports:

`show geaport`

Command mode: All

```
Logical Port  GEA Port(0-based)  GEA Unit
------------  -----------------  ---------
     1                1                0
     2                2                0
     3                4                0
     4                7                0
     5                8                0
     6               12                0
     7               13                0
     8               14                0
     9                0                0
    10                3                0
    11                5                0
    12                6                0
    13                9                0
    14               10                0
    15               11                0
    16               15                0
    17               16                0
    18               17                0
    19               18                0
    20               19                0
    21               23                0
    22               22                0
    23               21                0
    24               20                0
```

This display correlates the logical port number to the GEA unit on which each port resides.

Uplink Failure Detection information

The following table describes the commands used to display information about UFD (Uplink Failure Detection).

Table 33 UFD commands

Command	Usage
show ufd	Displays information for the current UFD. **Command mode:** All
show fdp *<1-4>*	Displays information for a FDP (Failure Detection Pair). **Command mode:** All
show ufd fdp ltd	Displays information for all LTD (Link to Disable). **Command mode:** All
show ufd fdp ltm	Displays information for all LTM (Link to Monitor). **Command mode:** All

The following command displays Uplink Failure Detection (UFD) information:

show ufd

Command mode: All

```
Uplink Failure Detection 1: Enabled
LtM status: Down
Member      STG    STG State       Link Status
---------   ---    ------------    -----------
  port 24                          down
             1       DISABLED
            10       DISABLED *
            15       DISABLED *
* = STP turned off for this port.

LtD status: Auto Disabled
Member       Link Status
---------    -----------
  port  1      disabled
  port  2      disabled
  port  3      disabled
  port  4      disabled

Uplink Failure Detection 2: Disabled

Uplink Failure Detection 3: Disabled

Uplink Failure Detection 4: Disabled
```

Uplink Failure Detection (UFD) information includes:

- UFD status, either enabled or disabled
- LtM status and member ports
- Spanning Tree status for LtM ports
- LtD status and member ports

Information dump

The following command dumps switch information:

show information-dump

Command mode: All

Use the dump command to dump all switch information available from this switch memory (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set the communication software on your workstation to capture session data prior to issuing the dump commands.

Statistics commands

Introduction

You can view switch performance statistics in the user, operator, and administrator command modes. This chapter discusses how to use the ISCLI to display switch statistics.

The following table describes general Statistics commands.

Table 34 Statistics commands

Command	Usage
show layer3 counters	Displays Layer 3 Statistics. **Command mode**: All
show snmp-server counters	Displays SNMP statistics. **Command mode**: All
show ntp counters	Displays Network Time Protocol (NTP) Statistics. You can execute the clear command option to delete all statistics. **Command mode**: All
clear ntp	Clears Network Time Protocol (NTP) Statistics. **Command mode**: All except User EXEC
show ufd counters	Displays Uplink Failure Detection statistics. **Command mode**: All
show counters	Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode**: All

Port Statistics

The following table describes the Port Statistics commands. The following sections provide more detailed information and commands.

Table 35 Port Statistics commands

Command	Usage
show interface gigabitethernet *<port number>* **bridging-counters**	Displays bridging (“dot1”) statistics for the port. **Command mode**: All
show interface gigabitethernet *<port number>* **ethernet-counters**	Displays Ethernet (“dot3”) statistics for the port. **Command mode**: All
show interface gigabitethernet *<port number>* **interface-counters**	Displays interface statistics for the port. **Command mode**: All
show interface gigabitethernet *<port number>* **ip-counters**	Displays Internet Protocol statistics for the port. **Command mode**: All
show interface gigabitethernet *<port number>* **link-counters**	Displays link statistics for the port. **Command mode**: All
show interface gigabitethernet *<port number>* **rmon-counters**	Displays RMON statistics for the port. **Command mode**: All

Bridging statistics

Use the following command to display the bridging statistics of the selected port:

show interface gigabitethernet *<port number>* **bridging-counters**

Command mode: All

```
Bridging statistics for port 1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

The following table describes the bridging statistics for a selected port:

Table 36 Bridging statistics for port

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. A frame transmitted on the interface corresponding to this port is counted by this object, if and only if, it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the forwarding process.
dot1TpLearnedEntryDiscards	The total number of Forwarding Database entries, which have been or would have been learned, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has adverse performance effects on the sub network). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

Ethernet statistics

Use the following command to display the ethernet statistics of the selected port:

show interface gigabitethernet *<port number>* **ethernet-counters**

Command mode: All

```
Ethernet statistics for port 1:
dot3StatsAlignmentErrors:                  0
dot3StatsFCSErrors:                        0
dot3StatsSingleCollisionFrames:            0
dot3StatsMultipleCollisionFrames:          0
dot3StatsLateCollisions:                   0
dot3StatsExcessiveCollisions:              0
dot3StatsInternalMacTransmitErrors:        0
dot3StatsFrameTooLongs:                    0
dot3StatsInternalMacReceiveErrors:         0
```

The following table describes the Ethernet statistics for a selected port:

Table 37 Ethernet statistics for port

Statistics	Description
dot3StatsAlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsSingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrame object.
dot3StatsMultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 37 Ethernet statistics for port

Statistics	Description
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsInternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

Interface statistics

Use the following command to display the interface statistics of the selected port:

show interface gigabitethernet *<port number>* **interface-counters**

Command mode: All

```
Interface statistics for port 1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
Discards:                          0                      0
Errors:                            0                  21187
```

The following table describes the interface (IF) statistics for a selected port:

Table 38 Interface statistics for port

Statistics	Description
Octets—IfHCIn	The total number of octets received on the interface, including framing characters.
UcastPkts—IfHCIn	The number of packets, delivered by this sublayer to a higher sublayer, which were not addressed to a multicast or broadcast address at this sublayer.
BroadcastPkts—IfHCIn	The number of packets, delivered by this sublayer to a higher sublayer, which were addressed to a broadcast address at this sublayer.
MulticastPkts—IfHCIn	The total number of packets, delivered by this sublayer. These are the packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both group and functional addresses.
Discards—IfHCIn	The number of inbound packets which were chosen to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Errors—IfHCIn	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Octets—IfHCOut	The total number of octets transmitted out of the interface, including framing characters.

Table 38 Interface statistics for port

Statistics	Description
UcastPkts—IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
BroadcastPkts—IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts.
MulticastPkts—IfHCOut	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both group and functional addresses. This object is a 64-bit version of ifOutMulticastPkts.
Discards—IfHCOut	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Errors—IfHCOut	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Internet Protocol (IP) statistics

Use the following command to display the interface protocol statistics of the selected port:

show interface gigabitethernet *<port number>* **ip-counters**

Command mode: All

```
GEA IP statistics for port 1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

The following table describes the Internet Protocol (IP) statistics for a selected port:

Table 39 IP statistics for port

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderError	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Link statistics

Use the following command to display the link statistics of the selected port:

show interface gigabitethernet *<port number>* **link-counters**

Command mode: All

```
Link statistics for port 1:
linkStateChange:              2
```

The following table describes the link statistics for a selected port:

Table 40 Link statistics for port

Statistic	Description
linkStateChange	The total number of link state changes.

Port RMON statistics

Use the following command to display the RMON statistics of the selected port:

show interface gigabitethernet *<port number>* **rmon-counters**

Command mode: All

```
RMON statistics for port 2:
etherStatsDropEvents:                        NA
etherStatsOctets:                             0
etherStatsPkts:                               0
etherStatsBroadcastPkts:                      0
etherStatsMulticastPkts:                      0
etherStatsCRCAlignErrors:                     0
etherStatsUndersizePkts:                      0
etherStatsOversizePkts:                       0
etherStatsFragments:                          0
etherStatsJabbers:                            0
etherStatsCollisions:                         0
etherStatsPkts64Octets:                       0
etherStatsPkts65to127Octets:                  0
etherStatsPkts128to255Octets:                 0
etherStatsPkts256to511Octets:                 0
etherStatsPkts512to1023Octets:                0
etherStatsPkts1024to1518Octets:               0
```

The following table describes the Remote Monitoring (RMON) statistics of the selected port:

Table 41 RMON statistics

Statistic	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Table 41 RMON statistics

Statistic	Description
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64 Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCSoctets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

Layer 2 statistics

The following table describes the Layer 2 statistics commands. The following sections provide more detailed information and commands.

Table 42 Layer 2 Statistics commands

Command	Usage
show mac-address-table counters	Displays the Forwarding Database statistics. **Command mode:** All
show interface gigabitethernet <*port number***> lacp counters**	Displays Link Aggregation Control Protocol (LACP) statistics. **Command mode**: All

FDB statistics

Use the following command to display statistics regarding the use of the forwarding database:

show mac-address-table counters

Command mode: All

```
FDB statistics:
 current:            91   hiwat:               91
```

These commands enable you to display statistics regarding the use of the forwarding database, including the number of current entries and the maximum number of entries ever recorded.

The following table describes the Forwarding Database (FDB) statistics:

Table 43 Forwarding Database statistics

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

LACP statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

show interface gigabitethernet <*port number***> lacp counters**

Command mode: All

```
Valid LACPDUs received         - 0
Valid Marker PDUs received     - 0
Valid Marker Rsp PDUs received - 0
Unknown version/TLV type       - 0
Illegal subtype received       - 0
LACPDUs transmitted            - 0
Marker PDUs transmitted        - 0
Marker Rsp PDUs transmitted    - 0
```

Layer 3 statistics

The following table describes basic Layer 3 statistics commands. The following sections provide more detailed information and commands. Layer 3 functionality is limited in this release.

Table 44 Layer 3 Statistics commands

Command	Usage
show ip counters	Displays IP statistics. **Command mode:** All except UserEXEC
clear ip counters	Clears IP statistics. Use this command with caution as it deletes all the IP statistics. **Command mode:** All except UserEXEC
show ip arp counters	Displays Address Resolution Protocol (ARP) statistics. **Command mode:** All except UserEXEC
show ip dns counters	Displays Domain Name System (DNS) statistics. **Command mode:** All except UserEXEC
show ip icmp counters	Displays ICMP statistics. **Command mode:** All except UserEXEC
show ip tcp counters	Displays Transmission Control Protocol (TCP) statistics. **Command mode:** All except UserEXEC
show ip udp counters	Displays User Datagram Protocol (UDP) statistics. Add the argument, clear, to clear UDP statistics. **Command mode:** All except UserEXEC
show ip igmp counters	Displays IGMP statistics. **Command mode:** All except UserEXEC
clear ip igmp *<1-4094>* **counters**	Clears all IGMP statistics for the selected VLANs. **Command mode:** All above Priv EXEC
show ip gea	Displays GEA statistics. **Command mode**: All except UserEXEC
show layer3 counters	Displays all Layer 3 statistics. **Command mode:** All

IP statistics

The following command displays IP statistics:

show ip counters

Command mode: All except User EXEC

```
IP statistics:
ipInReceives: 36475             ipInHdrErrors: 0
ipInAddrErrors: 905
ipInUnknownProtos: 0            ipInDiscards: 0
ipInDelivers: 4103              ipOutRequests: 30974
ipOutDiscards: 0
ipDefaultTTL: 255
```

The following table describes the IP statistics:

Table 45 IP statistics

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this switch. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Table 45 IP statistics

Statistics	Description
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this switch, whenever a TTL value is not supplied by the transport layer protocol.

ARP statistics

The following command displays Address Resolution Protocol statistics.

show ip arp counters

Command mode: All except User EXEC

```
ARP statistics:
arpEntriesCur:              2  arpEntriesHighWater:          4
```

The following table describes the Address Resolution Protocol (ARP) statistics:

Table 46 ARP statistics

Statistic	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.

DNS statistics

show ip dns counters

Command mode: All except User EXEC

```
DNS statistics:
dnsInRequests:              0  dnsOutRequests:             0
dnsBadRequests:             0
```

The following table describes the Domain Name System (DNS) statistics:

Table 47 DNS statistics

Statistic	Description
dnsInRequests	The total number of DNS request packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

ICMP statistics

The following command displays ICMP statistics:

show ip icmp counters

Command mode: All except User EXEC

```
ICMP statistics:
icmpInMsgs:              245802   icmpInErrors:               1393
icmpInDestUnreachs:          41   icmpInTimeExcds:               0
icmpInParmProbs:              0   icmpInSrcQuenchs:              0
icmpInRedirects:              0   icmpInEchos:                  18
icmpInEchoReps:          244350   icmpInTimestamps:              0
icmpInTimestampReps:          0   icmpInAddrMasks:               0
icmpInAddrMaskReps:           0   icmpOutMsgs:              253810
icmpOutErrors:                0   icmpOutDestUnreachs:          15
icmpOutTimeExcds:             0   icmpOutParmProbs:              0
icmpOutSrcQuenchs:            0   icmpOutRedirects:              0
icmpOutEchos:            253777   icmpOutEchoReps:              18
icmpOutTimestamps:            0   icmpOutTimestampReps:          0
icmpOutAddrMasks:             0   icmpOutAddrMaskReps:           0
```

The following table describes the Internet Control Messaging Protocol (ICMP) statistics:

Table 48 ICMP statistics

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the switch received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors	The number of ICMP messages which the switch received but determined as having ICMP specific errors (for example bad ICMP checksums and bad length).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this switch attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Table 48 ICMP statistics

Statistics	Description
icmpOutErrors	The number of ICMP messages that this switch did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

TCP statistics

The following command displays TCP statistics:

show ip tcp counters

Command mode: All except User EXEC

```
TCP statistics:
tcpRtoAlgorithm:          4   tcpRtoMin:               0
tcpRtoMax:           240000   tcpMaxConn:           2048
tcpActiveOpens:      252214   tcpPassiveOpens:         7
tcpAttemptFails:        528   tcpEstabResets:          4
tcpInSegs:           756401   tcpOutSegs:         756655
tcpRetransSegs:           0   tcpInErrs:               0
tcpCurBuff:               0   tcpCurConn:              3
tcpOutRsts:             417
```

The following table describes the Transmission Control Protocol (TCP) statistics:

Table 49 TCP statistics

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in Request For Comments (RFC) 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the switch can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Table 49 TCP statistics

Statistics	Description
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE- WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the reset (RST) flag.

UDP statistics

The following command displays UDP statistics:

`show ip udp counters`

Command mode: All except User EXEC

```
UDP statistics:
udpInDatagrams:         54   udpOutDatagrams:         43
udpInErrors:             0   udpNoPorts:         1578077
```

The following table describes the User Datagram Protocol (UDP) statistics:

Table 50 UDP statistics

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this switch.
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

IGMP Multicast Group statistics

The following command displays statistics about the use of the IGMP Multicast Groups:

show ip igmp counters

Command mode: All except User EXEC

```
------------------------------------------------------------
IGMP Snoop vlan 1 statistics:
------------------------------------------------------------
rxIgmpValidPkts:        0    rxIgmpInvalidPkts:             0
rxIgmpGenQueries:       0    rxIgmpGrpSpecificQueries:      0
rxIgmpLeaves:           0    rxIgmpReports:                 0
txIgmpReports:          0    txIgmpGrpSpecificQueries:      0
txIgmpLeaves:           0
```

These commands enable you to display statistics regarding the use of the IGMP Multicast Groups.

The following table describes the IGMP statistics:

Table 51 IGMP statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted

GEA Layer 3 statistics

The following table describes the Layer 3 GEA statistics commands.

Table 52 Layer 3 GEA statistics commands

Command	Usage
show ip gea bucket <*IP address***>**	Displays GEA statistics for a specific IP address. **Command mode**: All except User EXEC
show ip gea	Displays all GEA statistics. **Command mode**: All except User EXEC

GEA Layer 3 statistics

The following command displays GEA statistics:

show ip gea

Command mode: All except User EXEC

```
GEA L3 statistics:
         Max L3 table size                : 2048
         Number of L3 entries used        : 0

         Max LPM table size               : 256
         Number of LPM entries used       : 0
```

Management Processor statistics

The following table describes the MP-specific Statistics commands. The following sections provide more detailed information and commands.

Table 53 MP-specific Statistics commands

Command	Usage
show mp packet	Displays packet statistics, to check for leads and load. **Command mode**: All
show mp tcp-block	Displays all Transmission Control Protocol (TCP) control blocks (TCB) that are in use. **Command mode**: All
show mp udp-block	Displays all User Datagram Protocol (UDP) control blocks (UCB) that are in use. **Command mode**: All
show mp cpu	Displays CPU utilization for periods of up to 1, 4, and 64 seconds. **Command mode**: All

Packet statistics

The following command displays packet statistics:

show mp packet

Command mode: All

```
Packet counts:
 allocs:          36692     frees:                       36692
 mediums:             0     mediums hi-watermark:            3
 jumbos:              0     jumbos hi-watermark:             0
 smalls:              0     smalls hi-watermark:             2
 failures:            0
```

The following table describes the packet statistics.

Table 54 MP specific packet statistics

Description	Example statistic
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.

TCP statistics

The following command displays TCP statistics:

show mp tcp-block

Command mode: All

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0             0 <=> 0.0.0.0            80  listen
10ad5790:  47.81.27.5       1171 <=> 47.80.23.243       23  established
```

The following table describes the Transmission Control Protocol (TCP) control block (TCB) statistics shown in this example:

Table 55 MP specified TCP statistics

Description	Example statistic
Memory	10ad41e8/10ad5790
Destination IP address	0.0.0.0/47.81.27.5
Destination port	0/1171
Source IP	0.0.0.0/47.80.23.243
Source port	80/23
State	listen/established

UDP statistics

The following command displays UDP statistics:

show mp udp-block

Command mode: All

```
All UDP allocated control blocks:
  161:  listen
```

The following table describes the User Datagram Protocol (UDP) control block (UCB) statistics shown in this example:

Table 56 UDP statistics

Description	Example Statistic
Control block	161
State	listen

CPU statistics

The following command displays the CPU utilization statistics:

show mp cpu

Command mode: All

```
CPU utilization:
cpuUtil1Second:            8%
cpuUtil4Seconds:           9%
cpuUtil64Seconds:          8%
```

The following table describes the management port CPU utilization statistics:

Table 57 CPU statistics

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. This is shown as a percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. This is shown as a percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. This is shown as a percentage.

SNMP statistics

The following command displays SNMP statistics:

`show snmp-server counters`

Command mode: All

```
SNMP statistics:
snmpInPkts:                    54   snmpInBadVersions:              0
snmpInBadC'tyNames:             0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:             0   snmpEnableAuthTraps:            0
snmpOutPkts:                   54   snmpInBadTypes:                 0
snmpInTooBigs:                  0   snmpInNoSuchNames:              0
snmpInBadValues:                0   snmpInReadOnlys:                0
snmpInGenErrs:                  0   snmpInTotalReqVars:           105
snmpInTotalSetVars:             0   snmpInGetRequests:              2
snmpInGetNexts:                52   snmpInSetRequests:              0
snmpInGetResponses:             0   snmpInTraps:                    0
snmpOutTooBigs:                 0   snmpOutNoSuchNames:             2
snmpOutBadValues:               0   snmpOutReadOnlys:               0
snmpOutGenErrs:                 0   snmpOutGetRequests:             0
snmpOutGetNexts:                0   snmpOutSetRequests:             0
snmpOutGetResponses:           54   snmpOutTraps:                   0
snmpSilentDrops:                0   snmpProxyDrops:                 0
```

The following table describes the Simple Network Management Protocol (SNMP) statistics:

Table 58 SNMP statistics

Statistics	Description
`snmpInPkts`	The total number of messages delivered to the SNMP entity from the transport service.
`snmpInBadVersions`	The total number of SNMP messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
`snmpInBadC'tyNames`	The total number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the switch.
`snmpInBadC'tyUses`	The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation which was not allowed by the SNMP community named in the message.
`snmpInASNParseErrs`	The total number of ASN.1 (Abstract Syntax Notation One) or BER (Basic Encoding Rules), errors encountered by the SNMP protocol entity when decoding SNMP messages received. The Open Systems Interconnection (OSI) method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
`snmpEnableAuthTraps`	An object to enable or disable the authentication traps generated by this switch.
`snmpOutPkts`	The total number of SNMP messages which were passed from the SNMP protocol entity to the transport service.
`snmpInBadTypes`	The total number of SNMP messages which failed ASN.1 parsing.
`snmpInTooBigs`	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is too big.
`snmpInNoSuchNames`	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
`snmpInBadValues`	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.

Table 58 SNMP statistics

Statistics	Description
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is read-only. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value read-only in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is too big.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpOutReadOnlys	Not in use.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was too large.
snmpProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.

NTP statistics

The following command displays NTP statistics:

`show ntp counters`

Command mode: All

```
NTP statistics:
        Primary Server:
                Requests Sent:              17
                Responses Received:         17
                Updates:                    1
        Secondary Server:
                Requests Sent:              0
                Responses Received:         0
                Updates:                    0
        Last update based on response from primary server.
        Last update time: 18:04:16 Tue Mar 13, 2006
        Current system time: 18:55:49 Tue Mar 13, 2006
```

The switch uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time-calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following table describes the NTP statistics:

Table 59 NTP statistics

Statistics	Description
`Primary Server`	Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time. Responses Received: The total number of NTP responses received from the primary NTP server. Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
`Secondary Server`	Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. Responses Received: The total number of NTP responses received from the secondary NTP server. Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
`Last update based on response from primary server`	Last update of time on the switch based on either primary or secondary NTP response received.
`Last update time`	The time stamp showing the time when the switch was last updated.
`Current system time`	The switch system time when the command `show ntp counters` was issued.

Uplink Failure Detection statistics

The following command allows you to display Uplink Failure Detection (UFD) statistics.

`show ufd counters`

Command mode: All

```
Uplink Failure Detection statistics:
FDP number: 1
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 2
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 3
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
FDP number: 4
Number of times LtM link failure: 1
Number of times LtM link in Blocking State: 0
Number of times LtD got auto disabled: 1
```

The following table describes the Uplink Failure Detection (UFD) statistics:

Table 60 Uplink Failure Detection statistics

Statistic	Description
`Number of times LtM link failure`	The total numbers of times that link failures were detected on the uplink ports in the Link to Monitor group.
`Number of times LtM link in Blocking State`	The total number of times that Spanning Tree Blocking state was detected on the uplink ports in the Link to Monitor group.
`Number of times LtD got auto disabled`	The total numbers of times that downlink ports in the Link to Disable group were automatically disabled because of a failure in the Link to Monitor group.

Statistics dump

The following command dumps the switch statistics:

`show counters`

Use the dump command to dump all switch statistics available (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

Configuration Commands

Introduction

The Configuration commands are available only from an administrator login. They include commands for configuring every aspect of the switch. Changes can be saved to flash memory.

The following table describes the basic Configuration commands. The following sections provide more detailed information and commands.

Table 61 Configuration commands

Command	Usage
show running-config	Dumps current configuration to a script file. **Command mode**: All except User EXEC
copy running-config {ftp|tftp}	Backs up current configuration to FTP/TFTP server. **Command mode**: All except User EXEC
copy {ftp|tftp} running-config	Restores current configuration from FTP/TFTP server. **Command mode**: All except User EXEC

Viewing and saving changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply configuration changes when you use the ISCLI. Any changes are lost the next time the switch boots unless the changes are explicitly saved.

Saving the configuration

You must save configuration changes to flash memory, so the switch reloads the setting when you reset the switch.

IMPORTANT: If you do not save the changes, they are lost the next time the system is reloaded.

To save the new configuration, enter the following command at any prompt:

```
Switch# copy running-config startup-config
```

When you save configuration changes, the changes are saved to the active configuration block.

For instructions about selecting the configuration to run at the next system reload, see the “Selecting a configuration block” section in the “Boot Options” chapter.

System configuration

These commands allow you to configure switch management parameters such as user and administrator privilege mode passwords, browser-based management settings, and management access list.

The following table describes the System Configuration commands.

Table 62 System Configuration commands

Command	Usage
system date *<yyyy> <mm> <dd>*	Prompts the user for the system date. **Command mode**: Global configuration
system time *<hh>:<mm>:<ss>*	Configures the system time using a 24-hour clock format. **Command mode**: Global configuration
system timezone	Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc. **Command mode**: Global configuration
[no] system daylight	Disables or enables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled. **Command mode**: Global configuration
system idle *<1-60>*	Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 5 minutes. This setting affects both the console port and Telnet port. **Command mode**: Global configuration
[no] system notice *<1-1024 characters multi-line> <'-' to end>*	Displays login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines. **Command mode**: Global configuration
[no] banner *<1-80 characters>*	Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. **Command mode**: Global configuration
[no] hostname *<string>*	Enables or disables displaying of the host name (system administrator's name) in the command line interface. **Command mode**: Global configuration
[no] system bootp	Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default value is `enabled`. **Command mode**: Global configuration
[no] system dhcp	Enables or disables Dynamic Host Control Protocol for setting the management IP address on interface 256. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default value is `enabled`. **Command mode**: Global configuration
[no] enable password *<string>*	Allows administrators to assign the Privilege EXEC password. The password will be required to enter Privilege EXEC mode. The default value is `disabled`. **Command mode**: Global configuration
show system	Displays the current system parameters. **Command mode**: All except User EXEC

System host log configuration

The following table describes the Syslog Configuration commands.

Table 63 Syslog Configuration commands

Command	Description
[no] logging host *<1-2>* **address** *<IP address>*	Sets the IP address of the first or second syslog host. For example, 100.10.1.1 **Command mode**: Global configuration
logging host *<1-2>* **severity** *<1-7>*	Sets the severity level of the first or second syslog host displayed. The default is 7, which means log all the severity levels. **Command mode**: Global configuration
logging host *<1-2>* **facility** *<1-7>*	This option sets the facility level of the first or seconds syslog host displayed. The default is 0. **Command mode**: Global configuration
[no] logging console	Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default. **Command mode**: Global configuration
[no] logging log {*<feature>***}**	Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features or enable/disable syslog on all available features. Features include: • console • system • mgmt • cli • stg • vlan • ssh • ntp • ip • web • rmon • ufd • cfg **Command mode**: Global configuration
show logging	Displays the current syslog settings. **Command mode**: All

Secure Shell Server configuration

Telnet traffic on the network is not secure. These commands enable Secure Shell (SSH) access from any SSH client. The SSH program securely logs into another computer over a network and executes commands in a secure environment. All data using SSH is encrypted.

Secure Shell can be configured on the switch using the console port only. The commands are not available if you access the switch using Telnet or the Browser-based Interface (BBI).

NOTE: See the *Application Guide* for information on SSH.

The following table describes the SSHD Configuration commands.

Table 64 SSHD Configuration commands

Command	Description
ssh interval *<0-24>*	Defines interval for auto-generating the RSA server key. The switch will auto-generate the RSA server key at the interval defined in this command. The range is 0-24 hours. The value of zero (0) means the RSA server key auto-generation is disabled. If the switch has been busy performing any other key generation and the assigned time of interval expires, the RSA server will skip generating the key. **Command mode**: Global configuration
ssh scp-password	Defines the administrator password that is for Secure Copy (SCP) only. The username for this SCP administrator is *scpadmin*. Typically, SCP is used to copy files securely from one machine to another. In the switch, SCP is used to download and upload the switch configuration using secure channels. **Command mode**: Global configuration
ssh generate-host-key	Generates the RSA host keys manually. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). But you can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately. **Command mode**: Global configuration
ssh generate-server-key	Generates the RSA server key. The switch creates this key automatically while configuring the switch with Secure Shell (SSH). You can generate the key manually by using this command if you need to overwrite the key for security reasons. The command will take effect immediately. **Command mode**: Global configuration
ssh port *<TCP port number>*	Sets the SSH server port number. **Command mode**: Global configuration
ssh scp-enable	Enables the SCP apply and save. **Command mode**: Global configuration
no ssh scp-enable	Disables the SCP apply and save. This is the default for SCP. **Command mode**: Global configuration
ssh enable	Enables the SSH server. **Command mode**: Global configuration
no ssh enable	Disables the SSH server. This is the default for the SSH server. **Command mode**: Global configuration
show ssh	Displays the current SSH server configuration. **Command mode**: All except User EXEC

RADIUS server configuration

NOTE: See the *Application Guide* for information on RADIUS.

The following table describes the RADIUS Server Configuration commands.

Table 65 RADIUS Server Configuration commands

Command	Description
[no] radius-server primary-host *<IP address>* **key** *<1-32 characters>*	Sets the primary RADIUS server address and shared secret between the switch and the RADIUS server(s). **Command mode**: Global configuration
[no] radius-server secondary-host *<IP address>* **key** *<1-32 characters>*	Sets the secondary RADIUS server address and shared secret between the switch and the RADIUS server(s). **Command mode**: Global configuration
radius-server port *<UDP port number>*	Enter the number of the User Datagram Protocol (UDP) port to be configured, between 1500-3000. The default is 1645. **Command mode**: Global configuration
radius-server retransmit *<1-3>*	Sets the number of failed authentication requests before switching to a different RADIUS server. The range is 1-3 requests. The default is 3 requests. **Command mode**: Global configuration
radius-server timeout *<1-10>*	Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The range is 1-10 seconds. The default is 3 seconds. **Command mode**: Global configuration
[no] radius-server telnet-backdoor	Enables or disables the RADIUS back door for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when secure backdoor is enabled. **Command mode**: Global configuration
[no] radius-server secure-backdoor	Enables or disables the RADIUS back door using secure password for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when backdoor (`telnet`) is enabled. **Command mode**: Global configuration
radius-server enable	Enables the RADIUS server. **Command mode**: Global configuration
no radius-server enable	Disables the RADIUS server. This is the default. **Command mode**: Global configuration
show radius-server	Displays the current RADIUS server parameters. **Command mode**: All except User EXEC

IMPORTANT: If RADIUS is enabled, you must login using RADIUS authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using noradius and the administrator password even if the backdoor (`telnet`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`telnet ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this even if RADIUS servers are available.

If secure backdoor is enabled (`secbd ena`), type in `noradius` as a backdoor to bypass RADIUS checking, and use the administrator password to log into the switch. The switch allows this only if RADIUS servers are not available.

TACACS+ server configuration

TACACS+ (Terminal Access Controller Access Control System) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols are more secure than the TACACS encryption protocol. TACACS+ is described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports decoupled authentication, authorization, and accounting.

The following table describes the TACACS+ Server Configuration commands.

Table 66 TACACS+ Server Configuration commands

Command	Description
[no] tacacs-server primary-host *<IP address>* **key** *<1-32 characters>*	Defines the primary TACACS+ server address. **Command mode**: Global configuration
[no] tacacs-server secondary-host *<IP address>* **key** *<1-32 characters>*	Defines the primary or secondary shared secret between the switch and the TACACS+ server(s). **Command mode**: Global configuration
tacacs-server port *<TCP port number>*	Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49. **Command mode**: Global configuration
tacacs-server retransmit *<1-3>*	Sets the number of failed authentication requests before switching to a different TACACS+ server. The range is 1-3 requests. The default is 3 requests. **Command mode**: Global configuration
tacacs-server timeout *<4-15>*	Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The range is 4-15 seconds. The default is 5 seconds. **Command mode**: Global configuration
[no] tacacs-server telnet-backdoor	Enables or disables the TACACS+ back door for telnet. The `telnet` command also applies to SSH/SCP connections and the Browser-based Interface (BBI). The default is disabled. This command does not apply when secure backdoor (`secbd`) is enabled. **Command mode**: Global configuration
[no] tacacs-server secure-backdoor	Enables or disables the TACACS+ back door using secure password for telnet/SSH/ HTTP/HTTPS. The default is disabled. This command does not apply when backdoor (`telnet`) is enabled. **Command mode**: Global configuration
[no] tacacs-server privilege-mapping	Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`. **Command mode**: Global configuration
[no] tacacs-server user-mapping <*0-15***> {user|oper|admin}**	Maps a TACACS+ authorization level to this switch user level. Enter a TACACS+ privilege level (0-15), followed by the corresponding the user level (user, oper, admin). **Command mode**: Global configuration
tacacs-server enable	Enables the TACACS+ server. **Command mode**: Global configuration
no tacacs-server enable	Disables the TACACS+ server. This is the default. **Command mode**: Global configuration
show tacacs-server	Displays current TACACS+ configuration parameters. **Command mode**: All except User EXEC

IMPORTANT: If TACACS+ is enabled, you must login using TACACS+ authentication when connecting via the console or Telnet/SSH/HTTP/HTTPS. Backdoor for console is always enabled, so you can connect using `notacacs` and the administrator password even if the backdoor (`telnet`) or secure backdoor (`secbd`) are disabled.

If Telnet backdoor is enabled (`telnet ena`), type in `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this even if TACACS+ servers are available.

If secure backdoor is enabled (`secbd ena`), type in `notacacs` as a backdoor to bypass TACACS+ checking, and use the administrator password to log into the switch. The switch allows this only if TACACS+ servers are not available.

NTP server configuration

These commands enable you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

The following table describes the NTP Server Configuration commands.

Table 67 NTP Server Configuration commands

Command	Description
[no] ntp prisrv *<IP address>*	Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. For example, 100.10.1.1 **Command mode**: Global configuration
[no] ntp secsrv *<IP address>*	Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. For example, 100.10.1.2 **Command mode**: Global configuration
ntp interval *<1-44640>*	Specifies the interval, in minutes (1-44640), to resynchronize the switch clock with the NTP server. The default is 1440 seconds. **Command mode**: Global configuration
ntp enable	Enables the NTP synchronization service. **Command mode**: Global configuration
no ntp enable	Disables the NTP synchronization service. This is the default. **Command mode**: Global configuration
show ntp	Displays the current NTP service settings. **Command mode**: All

System SNMP configuration

The switch software supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

- SNMP parameters that can be modified include:
- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string

The following table describes the System SNMP Configuration commands. The following sections provide more detailed information and commands.

Table 68 System SNMP Configuration commands

Command	Description
[no] hostname *<1-64 characters>*	Configures the name for the system. The name can have a maximum of 64 characters. **Command mode**: Global configuration
[no] snmp-server location *<1-64 characters>*	Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode**: Global configuration
[no] snmp-server contact *<1-64 characters>*	Configures the name of the system contact. The contact can have a maximum of 64 characters. **Command mode**: Global configuration
snmp-server read-community *<1-32 characters>*	Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is *public*. **Command mode**: Global configuration
snmp-server write-community *<1-32 characters>*	Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is *private*. **Command mode**: Global configuration
snmp-server timeout *<1-30>*	Sets the timeout value for the SNMP state machine. The range is 1-30 minutes. The default value is 5 minutes. **Command mode**: Global configuration
[no] snmp-server authentication-trap enable	Enables or disables the use of the system authentication trap facility. The default setting is disabled. **Command mode**: Global configuration
[no] snmp-server link-trap <*1-24***> enable**	Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled. **Command mode**: Global configuration
[no] snmp-server ufd-trap	Enables or disables the sending of Uplink Failure Detection traps. The default setting is disabled. **Command mode**: Global configuration
show snmp-server	Displays the current SNMP configuration. **Command mode**: All

SNMPv3 configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please see RFC2271 to RFC2275.

The following table describes the SNMPv3 Configuration commands.

Table 69 SNMPv3 Configuration commands

Command	Description
snmp-server user *<1-16>*	Configures a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. The range is 1-16. **Command mode**: Global configuration
snmp-server view *<1-128>*	Configures different MIB views. The range is 1-128. **Command mode**: Global configuration
snmp-server access *<1-32>*	Configures access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. The range is 1-32. **Command mode**: Global configuration
snmp-server group *<1-16>*	Configures an SNMP group. A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. The range is 1-16. **Command mode**: Global configuration
snmp-server community *<1-16>*	Configures a community table entry. The community table contains objects for mapping community strings and version-independent SNMP message parameters. The range is 1-16. **Command mode**: Global configuration
snmp-server target-address *<1-16>*	Configures the destination address and user security levels for outgoing notifications. This is also called the transport endpoint. The range is 1-16. **Command mode**: Global configuration
snmp-server target-parameters *<1-16>*	Configures SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. The range is 1-16. **Command mode**: Global configuration
snmp-server notify *<1-16>*	Configures a notification index. A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. The range is 1-16. **Command mode**: Global configuration
snmp-server version {v1v2v3|v3only}	Enables or disables the access to SNMP version 1 and version 2. This command is enabled by default (v1v2v3). **Command mode**: Global configuration
show snmp-server v3	Displays the current SNMPv3 configuration. **Command mode**: All

SNMPv3 User Security Model configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

The following table describes the User Security Model Configuration commands.

Table 70 User Security Model Configuration commands

Command	Description
snmp-server user *<1-16>* **name** *<1-32 characters>*	Configures a string up to 32 characters long that represents the name of the user. This is the login name that you need in order to access the switch. **Command mode**: Global configuration
snmp-server user *<1-16>* **authentication-protocol {md5|sha|none} [authentication-password** *<password>***]**	Configures the authentication protocol and password. The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96, or none. The default algorithm is `none`. When you configure an authentication algorithm, you must provide a password, otherwise you receive an error message during validation. This command allows you to create or change your password for authentication. **Command mode**: Global configuration
snmp-server user *<1-16>* **privacy-protocol {des|none} [privacy-password** *<password>***]**	Configures the type of privacy protocol and the privacy password. The privacy protocol protects messages from disclosure. The options are `des` (CBC-DES Symmetric Encryption Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select `none` as the authentication protocol, you receive an error message. You can create or change the privacy password. **Command mode**: Global configuration
no snmp-server user *<1-16>*	Deletes the USM user entries. **Command mode**: Global configuration
show snmp-server v3 user	Displays the USM user entries. **Command mode**: All

SNMPv3 View configuration

The following table describes the SNMPv3 View Configuration commands.

Table 71 SNMPv3 View Configuration commands

Command	Description
snmp-server view *<1-128>* **name** *<1-32 characters>*	Defines the name for a family of view subtrees up to a maximum of 32 characters. **Command mode**: Global configuration
snmp-server view *<1-128>* **tree** *<1-64 characters>*	Defines the Object Identifier (OID), a string of maximum 64 characters, which when combined with the corresponding mask defines a family of view subtrees. An example of an OID is `1.3.6.1.2.1.1.1.0` **Command mode**: Global configuration
snmp-server view *<1-128>* **mask** *<1-32 characters>*	Defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. The mask can have a maximum of 32 characters. **Command mode**: Global configuration
snmp-server view *<1-128>* **type {included|excluded}**	Selects whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view. **Command mode**: Global configuration
no snmp-server view *<1-128>*	Deletes the `vacmViewTreeFamily` group entry. **Command mode**: Global configuration
show snmp-server v3 view	Displays the current `vacmViewTreeFamily` configuration. **Command mode**: All

SNMPv3 View-based Access Control Model configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

The following table describes the User Access Control Configuration commands.

Table 72 View-based Access Control Configuration commands

Command	Description
snmp-server access *<1-32>* **name** *<1-32 characters>*	Defines the name of the group, up to a maximum of 32 characters. **Command mode**: Global configuration
snmp-server access *<1-32>* **security {usm|snmpv1|snmpv2}**	Allows you to select the security model to be used. **Command mode**: Global configuration
snmp-server access *<1-32>* **level {noAuthNoPriv|authNo-Priv|authPriv}**	Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode**: Global configuration
snmp-server access *<1-32>* **read-view** *<1-32 characters>*	Defines a 32 character long read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode**: Global configuration
snmp-server access *<1-32>* **write-view** *<1-32 characters>*	Defines a 32 character long write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode**: Global configuration
snmp-server access *<1-32* **notify-view** *<1-32 characters>*	Defines a 32 character long notify view name that allows you notify access to the MIB view. **Command mode**: Global configuration
no snmp-server access *<1-32>*	Deletes the View-based Access Control entry. **Command mode**: Global configuration
show snmp-server v3 access	Displays the View-based Access Control configuration. **Command mode**: All

SNMPv3 Group configuration

The following table describes the SNMPv3 Group Configuration commands.

Table 73 SNMPv3 Group Configuration commands

Command	Description
snmp-server group *<1-16>* **security {usm|snmpv1|snmpv2}**	Defines the security model. **Command mode**: Global configuration
snmp-server group *<1-16>* **user-name** *<1-32 characters>*	Sets the user name. The user name can have a maximum of 32 characters. **Command mode**: Global configuration
snmp-server group *<1-16* **group-name** *<1-32 characters>*	The name for the access group. The group name can have a maximum of 32 characters. **Command mode**: Global configuration
no snmp-server group *<1-16>*	Deletes the `vacmSecurityToGroup` entry. **Command mode**: Global configuration
show snmp-server group *<1-16>*	Displays the current `vacmSecurityToGroup` configuration. **Command mode**: All

SNMPv3 Community Table configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

The following table describes the SNMPv3 Community Table Configuration commands.

Table 74 SNMPv3 Community Table Configuration commands

Command	Description
snmp-server community *<1-16>* **index** *<1-32 characters>*	Configures the unique index value of a row in this table. The index can have a maximum of 32 characters. **Command mode**: Global configuration
snmp-server community *<1-16>* **name** *<1-32 characters>*	Defines a readable 32 character string that represents the corresponding value of an SNMP community name in a security model. **Command mode**: Global configuration
snmp-server community *<1-16>* **user-name** *<1-32 characters>*	Sets the user name, up to 32 characters. **Command mode**: Global configuration
snmp-server community *<1-16>* **tag** *<1-255 characters>*	Configures a tag of up to 255 characters maximum. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode**: Global configuration
no snmp-server community *<1-16>*	Deletes the community table entry. **Command mode**: Global configuration
show snmp-server v3 community	Displays the community table configuration. **Command mode**: All

SNMPv3 Target Address Table configuration

These commands allow you to configure an entry of a transport address that transmits SNMP traps.

The following table describes the SNMPv3 Target Address Table Configuration commands.

Table 75 SNMPv3 Target Address Table Configuration commands

Command	Description
snmp-server target-address *<1-16>* **address** *< transport IP address>* **name** *<1-32 characters>*	Configures the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode**: Global configuration
snmp-server target-address *<1-16>* **name** *<1-32 characters>* **address** *<transport IP address>*	Configures a transport address IP that can be used in the generation of SNMP traps. **Command mode**: Global configuration
snmp-server target-address *<1-16>* **port** *<transport address port>*	Configures a transport address port that can be used in the generation of SNMP traps. **Command mode**: Global configuration
snmp-server target-address *<1-16>* **taglist** *<1-255 characters>*	Configures a list of tags (up to 255 characters maximum) that are used to select target addresses for a particular operation. **Command mode**: Global configuration
snmp-server target-address *<1-16>* **parameters-name** *<1-32 characters>*	Sets the parameter name. **Command mode**: Global configuration
no snmp-server target-address *<1-16>*	Deletes the Target Address Table entry. **Command mode**: Global configuration
show snmp-server v3 target-address	Displays the current Target Address Table configuration. **Command mode**: All

SNMPv3 Target Parameters Table configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthnoPriv`, `authNoPriv`, or `authPriv`).

The following table describes the SNMPv3 Target Parameters Table Configuration commands.

Table 76 SNMPv3 Target Parameters Table Configuration commands

Command	Description
snmp-server target-parameters *<1-16>* **name** *<1-32 characters*	Configures the locally arbitrary, but unique identifier that is associated with this entry. **Command mode**: Global configuration
snmp-server target-parameters *<1-16>* **message {snmpv1|snmpv2c|snmpv3}**	Configures the message processing model that is used to generate SNMP messages. **Command mode**: Global configuration
snmp-server target-parameters *<1-16>* **security {usm|snmpv1|snmpv2}**	Selects the security model to be used when generating the SNMP messages. **Command mode**: Global configuration
snmp-server target-parameters *<1-16>* **user-name** *<1-32 characters>*	Defines the name that identifies the user in the USM table, on whose behalf the SNMP messages are generated using this entry. **Command mode**: Global configuration
snmp-server target-parameters *<1-16>* **level {noAuthNo-Priv|authNoPriv|authPriv}**	Selects the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode**: Global configuration
no snmp-server target-parameters *<1-16>*	Deletes the `targetParamsTable` entry. **Command mode**: Global configuration
show snmp-server v3 target-parameters	Displays the current `targetParamsTable` configuration. **Command mode**: All

SNMPv3 Notify Table configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

The following table describes the SNMPv3 Notify Table Configuration commands.

Table 77 SNMPv3 Notify Table Configuration commands

Command	Description
snmp-server notify *<1-16>* **name** *<1-32 characters>*	Defines a locally arbitrary but unique identifier associated with this SNMP notify entry. **Command mode**: Global configuration
snmp-server notify *<1-16>* **tag** *<1-255 characters>*	Defines a tag of 255 characters maximum that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected. **Command mode**: Global configuration
no snmp-server notify *<1-16>*	Deletes the notify table entry. **Command mode**: Global configuration
show snmp-server v3 notify	Displays the current notify table configuration. **Command mode**: All

System Access configuration

The following table describes the System Access Configuration commands.

Table 78 System Access Configuration commands

Command	Description
[no] access http enable	Enables or disables HTTP (Web) access to the Browser-based Interface. It is enabled by default. **Command mode**: Global configuration
access http port *<TCP port number>*	Sets the switch port used for serving switch Web content. The default is HTTP port 80. **Command mode**: Global configuration
[no] access snmp {read-only| read-write}	Disables or provides read-only/write-read SNMP access. **Command mode**: Global configuration
[no] access telnet enable	Enables or disables telnet server. It is enabled by default. **Command mode**: Global configuration
access telnet port *<TCP port number>*	Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port. The default is 23. **Command mode**: Global configuration
access tftp-port *<TFTP port number>*	Sets an optional telnet server port number for cases where the server listens for TFTP sessions on a non-standard port. The default is 69. **Command mode**: Global configuration
show access	Displays the current system access parameters. **Command mode**: All except User EXEC

Management Networks configuration

The following table describes the Management Networks Configuration commands. You can configure up to 10 management networks on the switch.

Table 79 Management Networks Configuration commands

Command	Description
access management-network *<IP address> <IP mask>*	Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Command mode**: Global configuration
no access management-network *<IP address> <IP mask>*	Removes a defined network, which consists of a management network address and a management network mask address. **Command mode**: Global configuration
show access management-network	Displays the current management networks parameters. **Command mode**: All except User EXEC

User Access Control configuration

The following table describes the User Access Control commands.

Table 80 User Access Control Configuration commands

Command	Description
access user *<user name>*	Configures the User ID. **Command mode**: Global configuration
access user eject *<1-10>*	Ejects the selected user from the switch. Command mode: Global configuration
access user user-password *<1-128 characters>*	Sets the user (`user`) password (maximum of 128 characters). The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes. **Command mode**: Global configuration
access user operator-password *<1-128 characters>*	Sets the operator (`oper`) password (maximum of 128 characters). The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch. **Command mode**: Global configuration
access user administrator-password *<1-128 characters>*	Sets the administrator (`admin`) password (maximum of 128 characters). The super user administrator has complete access to all information and configuration commands on the switch, including the ability to change both the user and administrator passwords. **Command mode**: Global configuration
show access user	Displays the current user status. **Command mode**: All except User EXEC

User ID configuration

The following table describes the User ID Configuration commands.

Table 81 User ID Configuration commands

Command	Description
access user *<1-10>* **level {user|operator|administrator}**	Sets the Class-of-Service to define the user's authority level. **Command mode**: Global configuration
access user *<1-10>* **name** *<1-8 characters>*	Defines the user name of maximum eight characters. **Command mode**: Global configuration
access user *<1-10>* **password** *<1-128 characters>*	Sets the user password of up to 128 characters maximum. **Command mode**: Global configuration
access user *<1-10>* **enable**	Enables the user ID. **Command mode**: Global configuration
no access user *<1-10>* **enable**	Disables the user ID. **Command mode**: Global configuration
no access user *<1-10>*	Deletes the user ID. **Command mode**: Global configuration
show access user	Displays the current user ID parameters. **Command mode**: All except User EXEC

HTTPS Access configuration

The following table describes the HTTPS Access Configuration commands.

Table 82 HTTPS Access Configuration commands

Command	Description
[no] access https enable	Enables or disables BBI access (Web access) using HTTPS. The default value is `disabled`. **Command mode**: Global configuration
access https port *<TCP port number>*	Defines the HTTPS Web server port number. The default is 443. **Command mode**: Global configuration
access https generate-certificate	Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: • Country Name (2 letter code) [ ]: JP • State or Province Name (full name) [ ]: Tokyo • Locality Name (for example, city) [ ]: Fuchu • Organization Name (for example, company) [ ]: NEC • Organizational Unit Name (for example, section) [ ]: SIGMABLADE • Common Name (for example, user's name) [ ]: Taro • Email (for example, email address) [ ]: info@nec.com You must confirm if you want to generate the certificate. It takes approximately 30 seconds to generate the certificate. Then the switch restarts SSL agent. **Command mode**: Global configuration
access https save-certificate	Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted. **Command mode**: Global configuration
show access	Displays the current SSL Web Access configuration. **Command mode**: All except User EXEC

Port configuration

Use the port configuration commands to configure settings for individual switch ports.

NOTE: Port 19 is reserved for switch management interface.

The following table describes the Port Configuration commands. The following sections provide more detailed information and commands.

Table 83 Port Configuration commands

Command	Description
interface gigabitethernet *<port number>*	Enter Interface Port configuration mode for the selected port. **Command mode**: Global configuration
pvid *<1-4095>*	Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number for all ports except Port 19 is 1. Note: VLAN 4095 is reserved for switch management interface. **Command mode**: Interface port
name *<1-64 characters>*	Sets a name for the port (maximum 64 characters). The assigned port name displays next to the port number on some information and statistics screens. **Command mode**: Interface port
[no] rmon	Enables or disables Remote Monitoring for the port. The default is disabled. RMON must be enabled for any RMON configurations to function. **Command mode**: Interface port
[no] tagging	Disables or enables VLAN tagging for this port. It is disabled by default. **Command mode**: Interface port
[no] tag-pvid	Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is enabled. **Command mode**: Interface port
no shutdown	Enables the port. **Command mode**: Interface port
shutdown	Disables the port. To temporarily disable a port without changing its configuration attributes, see the “Temporarily disabling a port” section later in this chapter. **Command mode**: Interface port
show interface gigabitethernet *<port number>*	Displays current port parameters. **Command mode**: All

Temporarily disabling a port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Switch# interface gigabitethernet <port number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to perform a save operation. The port state reverts to its original configuration when the switch is reloaded.

Port link configuration

Use these commands to set port parameters for the port link.

Link commands are described in the following table. Using these commands, you can set port parameters such as speed, duplex, flow control, and negotiation mode for the port link.

The following table describes the Gigabit Link Configuration commands.

Table 84 Gigabit Link Configuration commands

Command	Description
speed {10|100|1000|auto}	Sets the link speed. Not all options are valid on all ports. The choices include: • 10 Mb/s • 100 Mb/s • 1000 Mb/s • "auto," for automatic detection (default) Note: Ports 1-18 are set to 1000 Mb/s, and cannot be changed. **Command mode**: Interface port
duplex {full|half|any}	Sets the operating mode. Not all options are valid on all ports. The choices include: • Full-duplex • Half-duplex • "Any," for automatic detection (default) Note: Ports 1-16 are set to "Any" and Ports 17-18 are set to full duplex. These ports cannot be changed. **Command mode**: Interface port
flowcontrol {receive|send|both}	Sets the flow control. The choices include: • Receive (rx) flow control • Transmit (tx) flow control • Both receive and transmit flow control (default) **Command mode**: Interface port
no flowcontrol	Sets the flow control to none. **Command mode**: Interface port
[no] auto	Enables or disables auto-negotiation for the port. The default is enabled. **Command mode**: Interface port
show interface gigabitethernet *<port number>*	Displays current port parameters. **Command mode**: All

Layer 2 configuration

The following table describes the Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 85 L2 Configuration commands

Command	Description
vlan *<1-4095>*	Enter VLAN configuration mode. **Command mode**: Global configuration
[no] spanning-tree uplinkfast	Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover. The default is disabled. **Note**: When enabled, this feature increases bridge priorities to 65500 for all STGs except STG 32 and path cost by 3000 for all external STP ports. **Command mode**: Global configuration
spanning-tree uplinkfast max-update-rate *<10-200>*	Configures the station update rate, in packets per second. The range is 10-200. The default value is 40. **Command mode**: Global configuration
show layer2	Displays current Layer 2 parameters. **Command mode**: All

Rapid Spanning Tree Protocol / Multiple Spanning Tree Protocol configuration

The switch supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

You can configure up to 31 spanning tree groups on the switch (STG 32 is reserved for switch management).

NOTE: When Multiple Spanning Tree is turned on, VLAN 1 is moved from Spanning Tree Group 1 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 1 is moved back to Spanning Tree Group 1.

The following table describes the Multiple Spanning Tree Configuration commands.

Table 86 Multiple Spanning Tree Configuration commands

Command	Description
[no] spanning-tree mstp name *<1-32 characters>*	Configures a name for the MSTP region. All devices within a MSTP region must have the same region name. **Command mode**: Global configuration
spanning-tree mstp version *<0-65535>*	Configures the revision level for the MSTP region. The revision level is used as a numerical identifier for the region. All devices within a MSTP region must have the same revision level number. The range is 0-65535. The default value is 1. **Command mode**: Global configuration
spanning-tree mstp maximum-hop *<4-60>*	Configures the maximum number of bridge hops a packet may to traverse before it is dropped. The range is from 4 to 60 hops. The default is 20. **Command mode**: Global configuration
spanning-tree mrst mode {mst|rstp|pvst}	Selects either Rapid Spanning Tree mode, as follows: • Rapid Spanning Tree mode (rstp) • Multiple Spanning Tree mode (mstp). • Per VLAN Spanning Tree (pvst) The default mode is pvst. **Command mode**: Global configuration
show spanning-tree mstp mrst	Displays the current RSTP/MSTP configuration. **Command mode**: All

NOTE:

- IEEE 802.1w standard-based RSTP implementation runs on one STG (i.e. same as one spanning tree instance) only. As a result, if 'rstp' mode is selected, then only a single RSTP instance (default for STG 1) is supported for all VLANs, including the Default VLAN 1.
- If multiple spanning tree instances are required, then select 'mstp' mode so that multiple VLANs are handled by multiple spanning tree instances, as specified by IEEE 802.1s standard-based MSTP implementation.
- IEEE 802.1s MSTP supports rapid convergence using IEEE 802.1w RSTP.
- PVST+ does not support rapid convergence in current versions.

NOTE:
The following configurations are unsupported:

- PVST+ (default Spanning Tree setting) is NOT interoperable with Cisco Rapid PVST+.
- MSTP/RSTP (with mode set to either 'mstp' or 'rstp') is NOT interoperable with Cisco Rapid PVST+.

The following configurations are supported:

- PVST+ (default Spanning Tree setting) is interoperable with Cisco PVST+.
- MSTP/RSTP (with mode set to 'mstp') is interoperable with Cisco MST/RSTP.

Common Internal Spanning Tree configuration

The Common Internal Spanning Tree (CIST) provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

The following table describes the commands used to configure CIST commands.

Table 87 CIST Configuration commands

Command	Description
spanning-tree mstp cist-add-vlan *<1-4095>*	Adds VLANs to the CIST. Enter one VLAN per line, and press Enter to add the VLANs. **Command mode**: Global configuration
default spanning-tree mstp cist	Resets all CIST parameters to their default values. **Command mode**: Global configuration
show spanning-tree mstp cist	Displays the current CIST configuration. **Command mode**: All

CIST bridge configuration

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+.

The following table describes the commands used to configure CIST Bridge Configuration commands.

Table 88 CIST Bridge Configuration commands

Command	Description
spanning-tree mstp cist-bridge priority *<0-65535>*	Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information. **Command mode**: Global configuration
spanning-tree mstp cist-bridge maximum-age *<6-40>*	Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information. **Command mode**: Global configuration
spanning-tree mstp cist-bridge forward-delay *<4-30>*	Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to RSTP. See the "Bridge Spanning Tree configuration" section for more information. **Command mode**: Global configuration
show spanning-tree mstp cist	Displays the current CIST bridge configuration. **Command mode**: All

CIST port configuration

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST.

For each port, CIST is turned on by default. Port parameters include:

- Port priority
- Port path cost
- Port Hello time
- Link type
- Edge
- On and off
- Current port configuration

The port option of MRST is turned on by default.

The following table describes the commands used to configure CIST Port Configuration commands.

Table 89 CIST Port Configuration commands

Command	Description
spanning-tree mstp cist interface-priority *<0-240>*	Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128. **Command mode**: Interface port
spanning-tree mstp cist path-cost *<0-200000000>*	Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 20000 for Gigabit ports. **Command mode**: Interface port
spanning-tree mstp cist hello *<1-10>*	Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds. **Command mode**: Interface port
spanning-tree mstp cist link-type {auto|p2p|shared}	Defines the type of link connected to the port, as follows: • auto: Configures the port to detect the link type, and automatically match its settings. • p2p: Configures the port for Point-To-Point protocol. • shared: Configures the port to connect to a shared medium (usually a hub). The default link type is auto. **Command mode**: Interface port
[no] spanning-tree mstp cist edge	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). By default, Ports 1-16 are configured as edge ports. **Command mode**: Interface port
spanning-tree mstp cist enable	Enables CIST on the port. Ports 17-18 and 20-24 are enabled by default. **Command mode**: Interface port
no spanning-tree mstp cist enable	Disables CIST on the port. **Command mode**: Interface port
show interface gigabitethernet *<port number>* **spanning-tree mstp cist**	Displays the current CIST port configuration. **Command mode**: All

Spanning Tree configuration

The switch supports the IEEE 802.1D Spanning Tree Protocol (STP) and Cisco proprietary PVST and PVST+ protocols. You can configure up to 31 spanning tree groups on the switch (STG 32 is reserved for switch management). Spanning Tree is turned on by default.

NOTE: When RSTP is turned on, only STP group 1 can be configured.

The following table describes the Spanning Tree Configuration commands.

Table 90 Spanning Tree Configuration commands

Command	Description
spanning-tree stp *<1-32>* **vlan** *<1-4095>*	Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter. **Command mode**: Global configuration
no spanning-tree stp *<1-32>* **vlan** *<1-4095>*	Breaks the association between a VLAN and a spanning tree and requires an external VLAN ID as a parameter. **Command mode**: Global configuration
no spanning-tree stp *<1-32>* **vlan all**	Removes all VLANs from a spanning tree. **Command mode**: Global configuration
spanning-tree stp *<1-32>* **enable**	Globally enables Spanning Tree Protocol. **Command mode**: Global configuration
no spanning-tree stp *<1-32>* **enable**	Globally disables Spanning Tree Protocol. **Command mode**: Global configuration
default spanning-tree *<1-32>*	Restores a spanning tree instance to its default configuration. **Command mode**: Global configuration
show spanning-tree stp *<1-32>*	Displays current Spanning Tree Protocol parameters. **Command mode**: All

Bridge Spanning Tree configuration

Spanning tree bridge parameters can be configured for each Spanning Tree Group. STP bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay
- Current bridge configuration

The following table describes the Bridge Spanning Tree Configuration commands.

Table 91 Bridge Spanning Tree Configuration commands

Command	Description
spanning-tree stp *<1-32>* **bridge priority** *<0-65535>*	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. RSTP/MSTP: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768. This command does not apply to MSTP. See the “Common Internal Spanning Tree configuration” section for more information. **Command mode**: Global configuration
spanning-tree stp *<1-32>* **bridge hello-time** *<1-10>*	Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds. This command does not apply to MSTP. See the “Common Internal Spanning Tree configuration” section for more information. **Command mode**: Global configuration
spanning-tree stp *<1-32>* **bridge maximum-age** *<6-40>*	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to MSTP. See the “Common Internal Spanning Tree configuration” section for more information. **Command mode**: Global configuration
spanning-tree stp *<1-32>* **bridge forward-delay** *<4-30>*	Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to MSTP. See the “Common Internal Spanning Tree configuration” section for more information. **Command mode**: Global configuration
show spanning-tree stp *<1-32>* **bridge**	Displays the current bridge STP parameters. **Command mode**: All

When configuring STP bridge parameters, the following formulas must be used:

- 2*(*fwd*-1) $\leq$ *mxage*
- 2*(*hello*+1) $\leq$ *mxage*

Spanning Tree port configuration

By default for STP/PVST+, Spanning tree is turned Off for downlink ports (1-16), and turned On for cross-connect ports (17-18), and uplink ports (20-24). By default for RSTP/MSTP, Spanning tree is turned Off for all downlink ports (1-16) configured as Edge ports, and turned On for cross-connect ports (17-18) and all uplink ports (20-24).

Spanning tree port parameters are used to modify STP operation on an individual port basis. STP port parameters include:

- Port priority
- Port path cost

The following table describes the Spanning Tree Port Configuration commands.

Table 92 Spanning Tree Port Configuration commands

Command	Description
spanning-tree stp *<1-32>* **priority** *<0-255>*	Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 255, and the default is 128. RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128. **Command mode**: Interface port
spanning-tree stp *<1-32>* **path-cost** *<0-200000000>*	Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The range is 0 to 65535. The default is 4 for Gigabit ports except Port 19. A value of 0 indicates that the default cost will be computed for an auto-negotiated link speed. The default cost is 19 for 100Mb/s ports and 4 for Gigabit ports. RSTP/MSTP: The range is 0 – 200000000, and the default is 20000 for Gigabit ports except Port 19. **Command mode**: Interface port
spanning-tree stp *<1-32>* **link {auto|p2p|shared}**	Defines the type of link connected to the port, as follows: auto: Configures the port to detect the link type, and automatically match its settings. p2p: Configures the port for Point-To-Point protocol. shared: Configures the port to connect to a shared medium (usually a hub). This command only applies when RSTP is turned on. See the "Common Internal Spanning Tree configuration" section for more information. **Command mode**: Interface port
[no] spanning-tree stp *<1-32>* **edge**	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). By default, Ports 1-16 are configured as edge ports. This command only applies when RSTP is turned on. See the "Common Internal Spanning Tree configuration" section for more information. **Command mode**: Interface port
[no] spanning-tree stp *<1-32>* **fastforward**	Enables or disables Port Fast Forward on the port. The default is disabled. **Command mode**: Interface port
spanning-tree stp *<1-32>* **enable**	Enables STP on the port. This is the default for Ports 17-18 and 20-24. **Command mode**: Interface port
no spanning-tree stp *<1-32>* **enable**	Disables STP on the port. Command mode: Interface port
show interface gigabitethernet *<port number>* **spanning-tree stp** *<1-32>*	Displays the current STP port parameters. **Command mode**: All

Forwarding Database configuration

The following table describes the Forwarding Database Configuration commands.

Table 93 FDB Configuration commands

Command	Description
mac-address-table aging <*0-65535***>**	Configures the aging value for FDB entries. The default value is 300. **Command mode**: Global configuration
show mac-address-table	Displays current FDB parameters. **Command mode**: All

Static FDB configuration

The following table describes the Static FDB Configuration commands.

Table 94 Static FDB Configuration commands

Command	Description
mac-address-table static *<MAC address> <VLAN> <port>*	Adds a static entry to the forwarding database. **Command mode**: Global configuration
no mac-address-table static [*<MAC address>***|***<VLAN>***]**	Deletes a static entry from the forwarding database. **Command mode**: Global configuration
mac-address-table static all [mac *<MAC address>***|vlan** *<VLAN>***|port** *<port>***]**	Clears specified static FDB entries from the forwarding database, as follows: • MAC address • VLAN • Port • All **Command mode**: Global configuration

Trunk configuration

Trunk groups can provide super-bandwidth connections between switches or other trunk capable devices. A trunk is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 12 trunk groups can be configured on the switch, with the following restrictions.

- Any physical switch port can belong to no more than one trunk group.
- Up to six ports/trunks can belong to the same trunk group.
- All ports in a trunk must have the same configuration for speed, flow control, and auto negotiation.
- Trunking from other devices must comply with Cisco® EtherChannel® technology.
- By default, port 17 and port 18 are trunked to support an internal switch-to-switch crosslink trunk. By default, ports 17 and 18 are disabled.

NOTE: See the *Application Guide* for information on how to use port trunks.

The following table describes the Trunk Group Configuration commands.

Table 95 Trunk Group Configuration commands

Command	Description
portchannel *<1-12>* **port** *<port number>*	Adds a physical port to the current trunk group. **Command mode**: Global configuration
no portchannel *<1-12>* **port** *<port number>*	Removes a physical port from the current trunk group. **Command mode**: Global configuration
portchannel *<1-12>* **enable**	Enables the current trunk group. **Command mode**: Global configuration
no portchannel *<1-12>* **enable**	Disables the current trunk group. **Command mode**: Global configuration
no portchannel *<1-12>*	Removes the current trunk group configuration. **Command mode**: Global configuration
show portchannel *<1-12>*	Displays current trunk group parameters. **Command mode**: All

Layer 2 IP Trunk Hash configuration

Trunk hash parameters are set globally for this switch. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

The following table describes the IP Trunk Hash Configuration commands.

Table 96 IP Trunk Hash Set commands

Command	Description
portchannel hash source-mac-address	Enable or disable trunk hashing on the source MAC. **Command mode**: Global configuration
portchannel hash destination-mac-address	Enable or disable trunk hashing on the destination MAC. **Command mode**: Global configuration
portchannel hash source-ip-address	Enable or disable trunk hashing on the source IP. **Command mode**: Global configuration
portchannel hash destination-ip-address	Enable or disable trunk hashing on the destination IP. **Command mode**: Global configuration
portchannel hash source-destination-ip	Enable trunk hashing on the source and destination IP. **Command mode**: Global configuration
portchannel hash source-destination-mac	Enable trunk hashing on the source and destination MAC address. **Command mode**: Global configuration
show portchannel hash	Display current trunk hash configuration. **Command mode**: All

Link Aggregation Control Protocol configuration

The following table describes the LACP Configuration commands.

Table 97 LACP Configuration commands

Command	Description
lacp system-priority <*1-65535***>**	Defines the priority value (1 through 65535) for the switch. Lower numbers provide higher priority. The default value is 32768. **Command mode**: Global configuration
lacp timeout {short|long}	Defines the timeout period before invalidating LACP data from a remote partner. Choose **short** (3 seconds) or **long** (90 seconds). The default value is **long**. **Command mode**: Global configuration
NOTE: We recommends that you use a timeout value of **long**, to reduce LACPDU processing. If your switch's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.	
show lacp	Display current LACP configuration. **Command mode**: All

LACP Port configuration

The following table describes the LACP Port Configuration commands.

Table 98 LACP Port Configuration commands

Command	Description
lacp mode {off|active|passive}	Set the LACP mode for this port, as follows: • **off** Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**. • **active** Turn LACP on and set this port to active. Active ports initiate LACPDUs. • **passive** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. **Command mode**: Inerface port
lacp priority <*1-65535***>**	Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 32768. **Command mode**: Inerface port
lacp key <*1-65535***>**	Set the admin key for this port. Only ports with the same admin key and oper key (operational state generated internally) can form a LACP trunk group. **Command mode**: Inerface port
show interface gigabitethernet <*port number***> lacp**	Displays the current LACP configuration for this port. **Command mode**: All

VLAN configuration

The commands in this section configure VLAN attributes, change the status of the VLAN, delete the VLAN, and change the port membership of the VLAN.

By default, the VLANs are disabled except VLAN 1 and 4095, which is always enabled. The switch supports a maximum of 1,000 VLANs. VLAN 4095 is reserved for switch management.

NOTE: See the *Application Guide* for information on VLANs.

The following table describes the VLAN Configuration commands.

Table 99 VLAN Configuration commands

Command	Description
vlan *<1-4095>*	Enter VLAN configuration mode. Command mode: Global configuration
name *<1-32 characters>*	Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. Command mode: VLAN configuration
stg *<0-32>*	Assigns a VLAN to a spanning tree group. STG number is assigned STGs 1-32 for STP/PVST+, only STG 1 for RSTP, and STGs 0-32 for MSTP (STG 0 is CIST). Command mode: VLAN configuration
member *<port number>*	Adds ports to the VLAN membership. Command mode: VLAN configuration
no member *<port number>*	Removes ports from the VLAN membership. Command mode: VLAN configuration
enable	Enables this VLAN. Command mode: VLAN configuration
no enable	Disables this VLAN without removing it from the configuration. Command mode: VLAN configuration
no vlan *<1-4095>*	Deletes this VLAN. Command mode: Global configuration
show vlan *<1-4095>*	Displays the current VLAN configuration. Command mode: All

IMPORTANT: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

Layer 3 configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands. Layer 3 functionality is limited in this release.

Table 100 L3 Configuration commands

Command	Description
interface ip *<1-256>*	Enter IP Interface mode. **Command mode**: Global configuration
show layer3	Displays the current IP configuration. **Command mode**: All except User EXEC

IP interface configuration

The switch can be configured with up to 256 IP interfaces. Each IP interface represents the switch on an IP subnet on your network. The IP Interface option is disabled by default. Interface 256 is reserved for switch management.

The following table describes the IP Interface Configuration commands.

Table 101 IP Interface Configuration commands

Command	Description
interface ip *<1-256>*	Enter IP interface mode. Command mode: Global configuration
ip address *<IP address> <IP netmask>*	Configures the IP address and mask of the switch interface using dotted decimal notation. Command mode: Interface IP
vlan *<1-4094>*	Configures the VLAN number for this interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it. Command mode: Interface IP
enable	Enables this IP interface. Command mode: Interface IP
no enable	Disables this IP interface. Command mode: Interface IP
no interface ip *<1-256>*	Removes this IP interface. Command mode: Global configuration
show interface ip *<1-256>*	Displays the current interface settings. Command mode: All

NOTE: If you enter an IP address for interface 1, you are prompted to change the BOOTP setting. Interface 256 is reserved for switch management interface.

Default Gateway configuration

The switch supports up to four gateways. By default, no gateways are configured on the switch. Enter 1, 2, 3, or 4 in the command as the <*gateway instance*>, depending upon which gateway you want to configure. Gateway 4 is reserved for switch management.

The following table describes the Default IP Gateway Configuration commands.

Table 102 Default IP Gateway Configuration commands

Command	Description
ip gateway *<1-4>* **address** *<IP address>*	Configures the IP address of the default IP gateway using dotted decimal notation. **Command mode**: Global configuration
ip gateway *<1-4>* **interval** *<0-60>*	The switch pings the default gateway to verify that it is up. This option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds. **Command mode**: Global configuration
ip gateway *<1-4>* **retry** *<1-120>*	Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts. **Command mode**: Global configuration
[no] ip gateway *<1-4>* **arp-health-check**	Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default. **Command mode**: Global configuration
ip gateway *<1-4>* **enable**	Enables the gateway for use. **Command mode**: Global configuration
no ip gateway *<1-4>* **enable**	Disables the gateway. **Command mode**: Global configuration
no ip gateway *<1-4>*	Deletes the gateway from the configuration. **Command mode**: Global configuration
show ip gateway *<1-4>*	Displays the current gateway settings. **Command mode**: All except User EXEC

NOTE: Gateway 4 is reserved for switch management interface.

Address Resolution Protocol configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

The following table describes the ARP Configuration commands.

Table 103 ARP Configuration commands

Command	Description
ip arp rearp <*2-120***>**	Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes. The default is 10 minutes. **Command mode**: Global configuration
show ip arp	Displays the current ARP configurations. **Command mode**: All except User EXEC

IGMP configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

IGMP snooping configuration

The following table describes the IGMP Snooping Configuration commands.

Table 104 IGMP Snooping commands

Command	Description
ip igmp snoop timeout *<1-255>*	Sets the Maximum Response Time (MRT) for IGMP hosts. MRT is one of the parameters used to determine the age out period of the IGMP hosts. Increasing the timeout increases the age out period. The range is from 1 to 255 seconds. The default is 10 seconds. **Command mode:** Global configuration
ip igmp snoop mrouter-timeout *<1-600>*	Configures the age-out period for the IGMP Mrouters in the Mrouter table. If the switch does not receive a General Query from the Mrouter for `mrto` seconds, the switch removes the multicast router from its Mrouter table. The range is from 1 to 600 seconds. The default is 255 seconds. **Command mode:** Global configuration
ip igmp snoop query-interval *<1-600>*	Sets the IGMP router query interval. The range is 1-600 seconds. The default value is 125. **Command mode:** Global configuration
ip igmp snoop robust *<2-10>*	Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), then increase the value. The default value is 2. **Command mode:** Global configuration
[no] ip igmp snoop aggregate	Enables or disables IGMP Membership Report aggregation. The default is enabled. **Command mode:** Global configuration
ip igmp snoop source-ip *<IP address>*	Configures the source IP address used as a proxy for IGMP Group Specific Queries. **Command mode:** Global configuration
ip igmp snoop vlan *<1-4094>*	Adds the VLAN to IGMP Snooping. **Command mode:** Global configuration
no ip igmp snoop vlan *<1-4094>*	Removes the VLAN from IGMP Snooping. **Command mode:** Global configuration
no ip igmp snoop vlan all	Removes all VLANs from IGMP Snooping. **Command mode:** Global configuration
[no] ip igmp snoop vlan *<1-4094>* **fast-leave**	Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default. **Command mode:** Global configuration
ip igmp snoop enable	Enables IGMP Snooping. **Command mode:** Global configuration
no ip igmp snoop enable	Disables IGMP Snooping. This is the default. **Command mode:** Global configuration
show ip igmp snoop	Displays the current IGMP Snooping parameters. **Command mode:** All except User EXEC

IGMP static multicast router configuration

The following table describes the Static Multicast Router Configuration commands.

NOTE: When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

Table 105 IGMP Static Multicast Router commands

Command	Description
ip igmp mrouter *<port number> <1-4094> <1-2>*	Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1 or 2) of the multicast router. **Command mode:** Global configuration
no ip igmp mrouter *<port number> <1-4094> <1-2>*	Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
show ip igmp mrouter	Displays the current IGMP Static Multicast Router parameters. **Command mode:** All except User EXEC

IGMP filtering configuration

The following table describes the IGMP Filter Configuration commands.

Table 106 IGMP Filtering commands

Command	Description
ip igmp filtering	Enables IGMP filtering globally. **Command mode:** Global configuration
no ip igmp filtering	Disables IGMP Filtering globally. This is the default. **Command mode:** Global configuration
show ip igmp filtering	Displays the current IGMP Filtering parameters. **Command mode:** All except User EXEC

IGMP filter definition

The following table describes the IGMP Filter Definition commands.

Table 107 IGMP Filter Definition commands

Command	Description
ip igmp profile *<1-16>* **range** *<IP multicast address> <IP multicast address>*	Configures the range of IP multicast addresses for this filter. Enter the first IP multicast address of the ranger, followed by the second IP multicast address of the range. **Command mode:** Global configuration
ip igmp profile *<1-16>* **action {allow|deny}**	Allows or denies multicast traffic for the IP multicast addresses specified. **Command mode:** Global configuration
ip igmp profile *<1-16>* **enable**	Enables this IGMP filter. **Command mode:** Global configuration
no ip igmp profile *<1-16>* **enable**	Disables this IGMP filter. This is the default. **Command mode:** Global configuration
no ip igmp profile *<1-16>*	Deletes this filter's parameter definitions. **Command mode:** Global configuration
show ip igmp profile *<1-16>*	Displays the current IGMP filter. **Command mode:** All except User EXEC

IGMP filtering port configuration

The following table describes the IGMP Port Filtering Configuration commands.

Table 108 IGMP Filtering Port commands

Command	Description
[no] ip igmp filtering	Enables or disables IGMP Filtering on this port. The default is disabled. **Command mode:** Interface port
ip igmp profile *<1-16>*	Adds an IGMP filter to this port. **Command mode:** Interface port
no ip igmp profile *<1-16>*	Removes an IGMP filter from this port. **Command mode:** Interface port
show interface gigabitethernet *<port number>* **igmp-filtering**	Displays the current IGMP filter parameters for this port. **Command mode:** All

Domain Name System configuration

The Domain Name System (DNS) Configuration commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the ping, traceroute, and tftp commands.

The following table describes the Domain Name System (DNS) Configuration commands.

Table 109 Domain Name System (DNS) Configuration commands

Command	Description
[no] ip name-server *<IP address>*	Sets the IP address for your primary DNS server. Use dotted decimal notation. **Command mode:** Global configuration
[no] ip name-server *<IP address>*	Sets the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation. **Command mode:** Global configuration
[no] ip domain-name *<string>*	Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
show ip dns	Displays the current Domain Name System (DNS) settings. **Command mode:** All except User EXEC

Remote Monitoring configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following table describes the RMON Configuration commands.

Table 110 RMON commands

Command	Description
show rmon	Displays the current RMON configuration. **Command mode:** All

RMON history configuration

The switch supports up to five History Groups.

The following table describes the RMON History commands.

Table 111 RMON History commands

Command	Description
rmon history *<1-65535>* **interface-oid** *<1-127 characters>*	Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: 1.3.6.1.2.1.2.2.1.1.x The interface OID can have a maximum of 127 characters. **Command mode:** Global configuration
rmon history *<1-65535>* **requested-buckets** *<1-65535>*	Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The range is from 1 to 65535. The default is 30. **Note**: The maximum number of buckets that can be granted is 50. **Command mode:** Global configuration
rmon history *<1-65535>* **polling-interval** *<1-3600>*	Configures the time interval over which the data is sampled for each bucket. The range is from 1 to 3600 seconds. The default value is 1800 seconds. **Command mode:** Global configuration
[no] rmon history *<1-65535>* **owner** *<1-127 characters>*	Enter a text string that identifies the person or entity that uses this history index. The owner can have a maximum of 127 characters. **Command mode:** Global configuration
no rmon history *<1-65535>*	Deletes the selected history group. **Command mode:** Global configuration
show rmon history	Displays the current RMON History parameters. **Command mode:** All

RMON event configuration

The switch supports up to 30 Event Groups.

The following table describes the RMON Event commands.

Table 112 RMON Event commands

Command	Description
rmon event *<1-65535>* **description** *<1-127 characters>*	Enter a text string to describe the event. The description can have a maximum of 127 characters. **Command mode:** Global configuration
[no] rmon event *<1-65535>* **type {log|trap|both}**	Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. **Command mode:** Global configuration
[no] rmon event *<1-65535>* **owner** *<1-127 characters>*	Enter a text string that identifies the person or entity that uses this event index. The owner can have a maximum of 127 characters. **Command mode:** Global configuration

Table 112 RMON Event commands

Command	Description
no rmon event *<1-65535>*	Deletes this event index. **Command mode:** Global configuration
show rmon event	Displays the current RMON Event parameters. **Command mode:** All

RMON alarm configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed. The switch supports up to 30 Alarm Groups.

The following table describes the RMON Alarm commands.

Table 113 RMON Alarm commands

Command	Description
rmon alarm *<1-65535>* **oid** *<1-127 characters>*	Configures an alarm MIB Object Identifier. The alarm OID can have a maximum of 127 characters. **Command mode:** Global configuration
rmon alarm *<1-65535>* **interval** *<1-65535>*	Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The range is from 1 to 65535 seconds. The default is 1800 seconds. **Command mode:** Global configuration
rmon alarm *<1-65535>* **sample {abs|delta}**	Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: abs: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. delta: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. The default is abs. **Command mode:** Global configuration
rmon alarm *<1-65535>* **alarm-type {rising|falling|either}**	Configures the alarm type as rising, falling, or either (rising or falling). The default is either. **Command mode:** Global configuration
rmon alarm *<1-65535>* **rising-limit** *<-2147483647 to 2147483647>*	Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. The default value is 0. **Command mode:** Global configuration
rmon alarm *<1-65535>* **falling-limit <***-2147483647 to 2147483647***>**	Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. The default value is 0. **Command mode:** Global configuration
rmon alarm *<1-65535>* **rising-crossing-index** *< 0-65535>*	Configures the rising alarm event index that is triggered when a rising threshold is crossed. The range is from 0 to 65535. The default value is 0. **Command mode:** Global configuration
rmon alarm *<1-65535>* **falling-crossing-index** *< 0-65535>*	Configures the falling alarm event index that is triggered when a falling threshold is crossed. The range is from 0 to 65535. The default value is 0. **Command mode:** Global configuration
[no] rmon alarm *<1-65535>* **owner** *<1-127 characters>*	Enter a text string that identifies the person or entity that uses this alarm index. The owner can have a maximum of 127 characters. **Command mode:** Global configuration
no rmon alarm *<1-65535>*	Deletes this alarm index. **Command mode:** Global configuration
show rmon alarm	Displays the current RMON Alarm parameters. **Command mode:** All

Port mirroring

Port Mirroring is used to configure, enable, and disable the monitored port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage. Port mirroring is disabled by default.

NOTE: See the “Troubleshooting tools” appendix in the *Application Guide* for information on how to use port mirroring.

The following table describes the Port Mirroring Configuration commands.

Table 114 Port Mirroring Configuration commands

Command	Description
[no] port-mirroring enable	Enables or disables port mirroring. The default is disabled. **Command mode:** Global configuration
show port-mirroring	Displays current settings of the mirrored and monitoring ports. **Command mode:** All

Port-based port mirroring

The following table describes the port-based Port Mirroring Configuration commands.

Table 115 Port Mirroring Configuration commands

Command	Description
port-mirroring monitor-port *<port number>* **mirroring-port** *<port number>* **{in|out|both}**	Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: • If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the mirrored port. • If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port. **Command mode:** Global configuration
no port-mirroring monitor-port *<port number>* **mirroring-port** *<port number>*	Removes the mirrored port. **Command mode:** Global configuration
no port-mirroring monitor-port *<port number>*	Deletes this monitor port. **Command mode:** Global configuration
show port-mirroring	Displays the current settings of the monitoring port. **Command mode:** All

Uplink Failure Detection configuration

Uplink Failure Detection (UFD) supports network fault tolerance in network adapter teams. Use these commands to configure a Failure Detection Pair of one Links to Monitor (LtM) group and one Links to Disable (LtD) group. When UFD is enabled and a Failure Detection Pair is configured, the switch automatically disables ports in the LtD if it detects a failure in the LtM. The failure conditions which are monitored in the LtM group include port link state moving to down, or port state moving to Blocking if Spanning Tree Protocol is enabled.

The following table describes the Uplink Failure Detection (UFD) Configuration commands.

Table 116 Uplink Failure Detection Configuration commands

Command	Description
ufd enable	Globally turns Uplink Failure Detection ON. **Command mode:** Global configuration
no ufd enable	Globally turns Uplink Failure Detection OFF. The default is OFF. **Command mode:** Global configuration
ufd fdp <*fdp number*>	Enter FDP configuration mode for the selected number. **Note:** This command is not available on the software version 1.0.0. **Command mode:** Global configuration
show ufd	Displays the current Uplink Failure Detection configuration parameters. **Command mode:** All

Failure Detection Pair configuration

Use these commands to configure a Failure Detection Pair, which consists of one Link to Monitor (LtM) and one Link to Disable (LtD). When the switch detects a failure on the LtM, it automatically disables the ports in the LtD.

The following table describes the Failure Detection Pair (FDP) configuration commands.

Table 117 Failure Detection Pair Configuration commands

Command	Description
enable	Enables the FDP Parameters. **Command mode:** FDP configuration
no enable	Disables the FDP Parameters. The default is disabled. **Command mode:** FDP configuration

Link to Monitor configuration

The following table describes the Link to Monitor (LtM) commands. The LtM can consist of only one uplink port (ports 20-24) a single trunk containing only uplink ports, or a single LACP trunk containing only uplink ports. The commands depend on the software version.

Table 118 Link to Monitor commands

Command	Description
ltm port *<port number>*	Adds a port to the LtM. Only uplink ports (20-24) are allowed in the LtM. **Command mode:** FDP configuration
no ltm port *<port number>*	Removes a port from the LtM. **Command mode:** FDP configuration
ltm portchannel *<1-12>*	Adds a trunk group to the LtM. The LtM trunk group can contain only uplink ports (20-24). **Command mode:** FDP configuration
no ltm portchannel *<1-12>*	Removes a trunk group from the LtM. **Command mode:** FDP configuration
ltm adminkey *<1-65535>*	Adds a LACP trunk group to the LtM. Defines a adminkey configured to a LACP trunk group. The LtM LACP trunk group can contain only uplink ports (20-24). **Command mode:** FDP configuration
no ltm adminkey *<1-65535>*	Removes a LACP trunk group from the LtM. **Command mode:** FDP configuration

Link to Disable configuration

The following table describes the Link to Disable (LtD) commands. The LtD can consist of any mix of downlink ports (ports 1-16) and trunk groups that contain only downlink ports and LACP trunk groups that contain only downlink ports. The commands depend on the software version.

Table 119 Link to Disable commands

Command	Description
ltd port *<port number>*	Adds a port to the current LtD group. Only downlink ports (1-16) are allowed in the LtD. **Command mode:** FDP configuration
no ltd port *<port number>*	Removes a port from the current LtD group. **Command mode:** FDP configuration
ltd portchannel *<1-12>*	Adds a trunk group to the current LtD group. LtD trunk groups can contain only downlink ports (1-16). **Command mode:** FDP configuration
no ltd portchannel *<1-12>*	Removes a trunk group from the current LtD group. **Command mode:** FDP configuration
ltd adminkey *<1-65535>*	Adds a LACP trunk group to the current LtD group. Defines a adminkey configured to a LACP trunk group. LtD LACP trunk groups can contain only downlink ports (1-16). **Command mode:** FDP configuration
no ltd adminkey *<1-65535>*	Removes a LACP trunk group from the current LtD group. **Command mode:** FDP configuration

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
Switch(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches. Paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via TFTP.

Saving the active switch configuration

When the **`copy running-config {ftp|tftp}`** command is used, the active configuration commands of the switch will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the prompt, enter:

```
Switch(config)# copy running-config {ftp|tftp}
```

NOTE: The output file is formatted with line-breaks but no carriage returns. The file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

NOTE: If the FTP/TFTP server is running SunOS™ or the Solaris™ operating system, the specified file must exist prior to executing the `copy running-config tftp` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Restoring the active switch configuration

When the **`copy {ftp|tftp} running-config`** command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial configuration.

To start the switch configuration download, at the prompt, enter:

```
Switch(config)#  copy {ftp|tftp} running-config
```

NOTE: The switch supports three configuration files: active, backup, and factory. See the “Selecting a configuration block” section in the “Boot Options” chapter for information on how to set which configuration file to use upon boot up.

Operations Commands

Introduction

Operations-level commands are used for making immediate and temporary changes to switch configuration. Operations commands are used for bringing ports temporarily in and out of service. These commands are available only from an administrator and operator login.

The following table describes basic Operations commands. The following sections provide more detailed information and commands.

Table 120 Operations commands

Command	Description
password	Allows the user to change the password. You need to enter the current password in use for validation. **Command mode**: All
clear logging	Clears all Syslog messages. This command is available only from an administrator login. **Command mode**: Privileged EXEC
ntp send	Allows the user to send requests to the NTP server. This command is available only from an administrator login. **Command mode**: Privileged EXEC

Operations-level port options

Operations-level port options are used for temporarily disabling or enabling a port.

Table 121 Operations-Level Port commands

Command	Description
[no] interface gigabitethernet *<port number>* **rmon**	Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function. **Command mode**: All
no interface gigabitethernet *<port number>* **shutdown**	Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reloaded. **Note**: This command does not enable a port that has been disabled by an ekeying mismatch error. **Command mode**: All
interface gigabitethernet *<port number>* **shutdown**	Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reloaded. **Command mode**: All
show interface gigabitethernet *<port number>* **operation**	Displays the current settings for the port. **Command mode**: All

Boot Options

Introduction

You must be logged in to the switch as the administrator to use the Boot Options commands.

The Boot Options allow you to perform the following functions:

- Select a switch software image to be used when the switch is next reloaded.
- Select a configuration block to be used when the switch is next reloaded.
- Download or upload a new software image to the switch via FTP/TFTP.

Each of the Boot Options commands is discussed in the following sections.

Updating the switch software image

The switch software image is the executable code running on the switch. A version of the image ships with the switch, and comes pre-installed on the switch. As new versions of the image are released, you can upgrade the software running on the switch.

To upgrade the software image on the switch:

- Load the new image onto a FTP/TFTP server on your network.
- Download the new image from the FTP/TFTP server to the switch.
- Select the new software image to be loaded into switch memory the next time the switch is reloaded.

Downloading new software to the switch

The switch can store up to two different software images, called image1 and image2, as well as boot software, called boot. When you download new software, you must specify where it should be placed: either into image1, image2, or boot.

By default, the software for the Layer2 switch mode (NormalPanel) is stored in the image1, and the software for the SmartPanel mode is stored in the image2.

To download new software to the switch, you need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The name of the new software image or boot file

NOTE: The DNS parameters must be configured if specifying hostnames. See the “Domain name system configuration” section in the “Configuration Commands” chapter.

NOTE: For the information of SmartPanel, see the SmartPanel and Reference Guide.

When the above requirements are met, use the following procedure to download the new software to the switch.

1. In Privileged EXEC mode, enter:

```
Switch# copy tftp {image1|image2|boot-image}
```

or

```
Switch# copy ftp {image1|image2|boot-image}
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IP address of the FTP/TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <server name or IP
address>
```

4. Enter the name of the new software file on the server:

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by FTP/TFTP server. However, the file location is normally relative to the FTP/TFTP directory.

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. The system prompts you to confirm your request.

   You should next select a software image to run, as described in the “Selecting a Soft Image to Run” section.

8. If you are loading an image from which you are not currently booted, the system prompts you to change the image.

```
image2 currently contains Software Version 1.1.0
 that was downloaded at 15:46:36 Wed Apr 23, 2006.
New download will replace image2 with file "1.1.0_OS.img"
 from TFTP server 192.168.2.4.
Confirm download operation [y/n]: y
Invoking TFTP over port 69...
Starting download...
File appears valid
Download in
progress..................................................
Image download complete (1333953 bytes)
Writing to flash...This takes about 90 seconds. Please wait
Write complete (1333953 bytes), now verifying FLASH...
Verification of new image2 in FLASH successful.
image2 now contains Software Version 1.1.0
Switch is currently set to boot software image1.
Do you want to change that to the new image2? [y/n] y
Next boot will use new software image2.
```

Selecting a software image to run

You can select which software image (image1 or image2) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
Switch(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.

Specify new image to use on next reset ["image1"/"image2"]:
```

IMPORTANT: When the switch software is changed (NormalPanel or SmartPanel) and the switch is rebooted, the switch configuration is removed and the switch runs factory configuration block. Backup the switch configuration if needed.

Uploading a software image from the switch

You can upload a software image from the switch to a FTP/TFTP server.

1. In Privileged EXEC mode, enter:

```
Switch# copy {image1|image2|boot-image} tftp
```

   or

```
Switch# copy {image1|image2|boot-image} ftp
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded

["image1"|"image2"|"boot"]: <image>
```

3. Enter the name or the IP address of the FTP/TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <server name or IP
address>
```

4. Enter the name of the file into which the image will be uploaded on the FTP/TFTP server:

```
Enter name of file on FTP/TFTP server: <filename>
```

5. Enter the user name, if you are using a FTP server:

```
Enter username for FTP server or hit return for TFTP server: <userID>
```

6. Enter the password for the FTP server (if prompted):

```
Enter password for username on FTP server: <password>
```

7. The system then requests confirmation of what you have entered. To have the file uploaded, enter y.

```
image2 currently contains Software Version 1.1.0
Upload will transfer image2 (1889411 bytes) to file "test"
 on TFTP server 192.1.1.1.
Confirm upload operation [y/n]: y
```

Selecting a configuration block

When you make configuration changes to the switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you execute a save operation (**copy running-config startup-config**), your new configuration changes are placed in the active configuration block. The previous configuration is copied into the backup configuration block.

There is also a factory configuration block. This holds the default configuration set by the factory when the switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured switch is moved to a network environment where it will be re-configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. In Global Configuration mode, enter:

```
Switch(config)# boot configuration-block {active|backup|factory}
```

2. Enter the name of the configuration block you want the switch to use.

   The system indicates which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.

Specify new block to use ["active"/"backup"/"factory"]:
```

Resetting the switch

You can reset the switch to make your software image file and configuration block changes occur.

Resetting the switch causes the Spanning Tree Protocol to restart. This process can be lengthy, depending on the topology of your network.

To reset the switch, at the prompt, enter:

```
>> Switch# reload
```

You are prompted to confirm your request.

Accessing the AOS CLI

To access the AOS CLI, enter the following command from the ISCLI, and reload the switch:

```
>> Switch(config)# boot cli-mode aos
```

The default command-line interface for this switch is the AOS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

Users can select the CLI mode upon login, if the following command is enabled:
`boot cli-mode prompt`

Only an administrator connected through the console port can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

Current switch software information

To display the current switch software information, enter the following.

```
>> Boot Options# cur
Currently set to boot software image2, factory default config block.
Current FLASH software:
  image1: version 1.2.0, downloaded  0:15:51 Mon Jan  2, 2006
          NormalPanel
  image2: version 1.0.0, downloaded  1:32:08 Sun Jan  8, 2006
          SmartPanel
  boot kernel: version 1.2.0
```

Use this command to display the image running on the switch, the Configuration block which the switch runs after booted, and the switch software stored in image1 and image2.

When NormalPanel is displayed in the software information, the software for Layer2 switch mode is stored in the image. When SmartPanel is displayed, the software for SmartPanel mode is stored in the image.

Maintenance Commands

Introduction

The Maintenance commands are used for debugging purposes, enabling you to generate a technical support dump of the critical state information in the switch, and to clear entries in the Forwarding Database and the Address Resolution Protocol (ARP) and routing tables. These commands are available only from an administrator login.

Dump information contains internal switch state data that is written to flash memory on the switch after any one of the following occurs:

- The switch administrator forces a switch panic. The panic option causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- The switch administrator enters the switch reset key combination (`Ctrl-Shift-6`) on a device that is attached to the console port.
- The switch detects a hardware or software problem that requires a reboot.

The following sections provide detailed information and commands.

System maintenance

The System Maintenance commands are reserved for use by NEC technical support. The options are used to perform system debugging.

The following table describes the System Maintenance commands.

Table 122 System Maintenance commands

Command	Usage
debug debug-flags	Sets the flags that are used for debugging purposes by NEC technical support. **Command mode:** All except User EXEC

Forwarding Database maintenance

The Forwarding Database (FDB) Manipulation commands can be used to view information and to delete a MAC address from the Forwarding Database or clear the entire Forwarding Database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

The following table describes the FDB Manipulation commands.

Table 123 FDB Manipulation commands

Command	Usage
show mac-address-table address *<MAC address>*	Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using one of the following: • xx:xx:xx:xx:xx:xx format (for example: 08:00:20:12:34:56) • xxxxxxxxxxxx format (for example: 080020123456). **Command mode:** All
show mac-address-table port *<port number>*	Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table vlan *<1-4095>*	Displays all FDB entries on a single VLAN. **Command mode:** All
show mac-address-table	Displays all entries in the Forwarding Database. **Command mode:** All
clear mac-address-table	Clears the entire Forwarding Database from switch memory, then adds the static entries to the Forwarding Database. **Command mode:** All except User EXEC

Debugging options

The Miscellaneous Debug commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using Debug commands:

- Events traced by the management processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the management processor (MP) trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by NEC technical support.

The following table describes the Miscellaneous Debug commands:

Table 124 Miscellaneous Debug commands

Command	Usage
debug mp-trace	Displays the management processor trace buffer. Header information similar to the following is shown: MP trace buffer at 13:28:15 Fri May 25, 2002; mask: 0x2ffdf748 The buffer information is displayed after the header. **Command mode:** All except User EXEC
debug mp-snap	Displays the management processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. **Command mode:** All except User EXEC
clear flash-config	Deletes all flash configuration blocks. The next time the switch is rebooted, it returns to the factory default settings. **Command mode:** All except User EXEC

ARP cache maintenance

The following table describes the Address Resolution Protocol commands:

Table 125 ARP Maintenance commands

Command	Usage
show ip arp find *<IP address>*	Shows a single ARP entry by IP address. **Command mode:** All except User EXEC
show ip arp interface *<port number>*	Shows ARP entries on a single port. **Command mode:** All except User EXEC
show ip arp vlan *<1-4095>*	Shows ARP entries on a single VLAN. **Command mode:** All except User EXEC
show ip arp reply	Shows the list of IP addresses that the switch will respond to for ARP requests. **Command mode:** All except User EXEC
show ip arp	Shows all ARP entries. **Command mode:** All except User EXEC
clear ip arp-cache	Clears the entire ARP list from switch memory. **Command mode:** All except User EXEC

NOTE: To display all ARP entries currently held in the switch, or a portion according to one of the commands listed above, see the “ARP information” section of the “Information Commands” chapter.

IGMP Snooping maintenance

The following table describes the IGMP Snooping Maintenance commands.

Table 126 IGMP Snooping Maintenance commands

Command	Usage
show ip igmp groups address *<IP address>*	Shows a single IGMP Multicast group by IP address. **Command mode:** All except User EXEC
show ip igmp groups vlan *<1-4094>*	Shows IGMP Multicast groups on a single VLAN. **Command mode:** All except User EXEC
show ip igmp groups interface *<port number>*	Shows IGMP Multicast groups on a single port. **Command mode:** All except User EXEC
show ip igmp groups	Shows all IGMP Multicast groups. **Command mode:** All except User EXEC
clear ip igmp snoop	Clears IGMP Multicast data from switch memory. **Command mode:** All except User EXEC

IGMP Mrouter maintenance

The following table describes the IGMP Multicast Routers Maintenance commands.

Table 127 IGMP Multicast Group Maintenance commands

Command	Usage
show ip igmp groups vlan *<1-4094>*	Shows IGMP Multicast groups on a single VLAN. **Command mode:** All except User EXEC
show ip igmp mrouter	Shows all IGMP Multicast routers. **Command mode:** All except User EXEC
clear ip igmp mrouter	Clears IGMP Multicast router data from switch memory. **Command mode:** All except User EXEC

Technical support dump

show tech-support

Command mode: All

Use the dump command to dump all switch information, statistics, and configuration for technical support.

If you want to capture dump data to a file, set the communication software on your workstation to capture session data prior to issuing the dump commands.

FTP/TFTP technical support dump put

Use this command to put (save) the technical support dump to a FTPTFTP server.

To save dump information via TFTP, at the prompt, enter:

```
Switch# copy tech-support tftp
```

or

To save dump information via FTP, at the prompt, enter:

```
Switch# copy tech-support ftp
```

The system prompts you to enter the server IP address or hostname, and the target dump file name.

Uuencode flash dump

show flash-dump-uuencode

Command mode: All

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the command. This will ensure that you do not lose any information. Once entered, the command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the above command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see the "Clearing dump information" section later in this chapter.

To access dump information, at the prompt, enter:

```
Switch# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following displays:

```
No FLASH dump available.
```

FTP/TFTP system dump put

Use this command to put (save) the system dump to a FTP/TFTP server.

NOTE: If the TFTP server is running SunOS or the Solaris operating system, the specified **copy flash-dump tftp** (or ftp) file must exist prior to executing the **copy flash-dump tftp** command (or **copy flash-dump tftp**) command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, at the prompt, enter:

```
Switch# copy flash-dump tftp <server> <filename>
```

or

To save dump information via FTP, at the prompt, enter:

```
Switch# copy flash-dump ftp
```

The system prompts you to enter the server IP address or hostname, and the target dump file name.

Clearing dump information

To clear dump information from flash memory, at the prompt, enter:

```
Switch# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Panic command

The panic command causes the switch to dump state information immediately to flash memory and reboot.

To select panic, at the prompt, enter:

```
>> Switch# debug panic
A FLASH dump already exists.
Confirm replacing existing dump and reboot [y/n]:
```

Enter **y** to confirm the command:

```
Dump and reboot [y/n]: y
```

A list of messages is displayed:

```
Starting system dump...done.

Reboot at 11:54:08 Wednesday October 30, 2006...

. . . . . .

. . . . . .

Rebooted because of console PANIC command.

Booting complete
```

Unscheduled system dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday October 30, 2006.
      Use show flash-dump uuencode to
      extract the dump for analysis and clear flash-dump to
     clear the FLASH region. The region must be cleared
     before another dump can be saved.
```